

TITLE:	CYBER SECURITY PLANNING		
POLICY #:	P-CCSP-001	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



State of Colorado Cyber Security Policies

Cyber Security Planning

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.

Cyber Security in the State of Colorado's distributed IT operational environment has proven to be vastly different based on each Agency's interpretation of the need and impact of Cyber Security. The State of Colorado Cyber Security Policies serve to provide a consistent framework by which all Agencies can describe and manage their Cyber Security Programs.

Authority

C.R.S. 24-37.5-401, C.R.S. 24-37.5-403, C.R.S. 24-37.5-404, C.R.S. 24-37.5-405,
C.R.S. 24-37.5-406

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

It is the policy of State of Colorado to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse or theft of sensitive electronic information assets. Each Agency throughout the State of Colorado shall maintain a Cyber Security Program to control risks associated with access, use, storage and sharing of sensitive citizen and State electronic

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:	CYBER SECURITY PLANNING		
POLICY #:	P-CCSP-001	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



information, and document the program details in an Agency Cyber Security Plan (ACSP). At a minimum, each ACSP shall include the following elements:

- Incident Response
- IT Risk Management Plan
- Disaster Recovery
- Vendor Management
- Network Operations
- Systems and Application Security
- Access Controls
- Change Control and Configuration Management
- Physical Security
- Data Handling and Disposal
- Personnel Security
- Acceptable Use
- Online Privacy
- Training and Awareness
- Security Review and Audit
- Security Metrics

To carry out this plan, the Agency shall appoint to the position of Information Security Officer (ISO) an Agency staff member or contractor who has appropriate cyber security experience and Agency IT environment knowledge.

The State CISO shall annually review and approve, conditionally approve, or disapprove each Agency Cyber Security Plan based on evaluation of the Plan and supporting documentation.

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

State CISO – is responsible for:

- Establishing and maintaining the Colorado Cyber Security Program, which provides guidance at an organizational level for the State Agency IT Organizations.
- Reviewing Agency Cyber Security Plan approval packages submitted by the Executive Directors.
- Reviewing and/or revising an Agency’s Plan of Action and Milestones.

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:	CYBER SECURITY PLANNING		
POLICY #:	P-CCSP-001	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



Agency Executive Director – is responsible for ensuring sufficient funding to accommodate the role of the Agency ISO and providing the necessary organizational support to the Agency ISO.

Agency Chief Information Officer (CIO) – is responsible for delegating the cyber security responsibilities to a staff member and ensuring the appropriate level of support for the associated duties in Agency Policy.

Agency ISO – is responsible for the organization and operation of the agency Information Security Operations.

Requirements

Cyber Security Plan

An Agency Cyber Security Plan (ACSP) shall include the following sections, at a minimum:

- I. Agency Mission Objectives
 - a. Mission Statement
Summarize or insert the Agency Mission Statement
 - b. Concept of Operations
Describe the operational goals of the Cyber Security Program and the conceptual functions that are implemented to achieve these goals.
 - c. Roles and Responsibilities
Identify responsibilities for implementing, monitoring, and managing the Cyber Security Program, specifically including the responsibilities of the Executive Director, Agency CIO, Security Staff, Agency IT staff, Agency Human Resources staff, and Agency staff.

- II. Information Technology Environment
 - a. Network Environment, Enclaves, and Perimeters
Describe the current network environment in detail, including characterizing of network segments into Security Enclave and identify the perimeters of each Security Enclave.
 - b. Critical Systems
List Agency critical systems by name, function, and the network segments they reside on.
 - c. General Support Systems
Define general support systems as they pertain to the environment (e.g., Active Directory Domains/Forests, NIS+ domains, or e-mail systems).

- III. Risk Management

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:	CYBER SECURITY PLANNING		
POLICY #:	P-CCSP-001	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.

- a. **Risk Assessment Methodology**
Describe the methodologies used for formal and informal System-level and Agency-wide Risk Assessments and the process for initiating a Risk Assessment, mitigating unacceptable risk, approving residual risk, and updating existing Risk Acceptance. Include the identification of the individual responsible for accepting residual risk.
- b. **Risk Assessment Responsibilities**
Identify any responsibilities in the Risk Management function that are outside the scope of the Roles and Responsibilities section of the ACSP.
- c. **Risk Assessment Frequency**
Identify the maximum length of time between System-level and Agency-wide Risk Assessments.
- d. **Project Lifecycle**
Describe how the Risk Management strategy is integrated into System, Network, and Application engineering project lifecycles, specifically identifying control points that trigger Risk Management activities.
- e. **Vendor Management**
Describe the role of Risk Management in the assessment, selection, and management of IT service providers or vendors.

IV. Security Program

- a. **Network Operations**
Describe standards for Network Operations as they pertain to Network Access Controls, Perimeter Security, Network Administration, Monitoring and Reporting, and Network Device Inventory.
- b. **System and Application Security**
Describe standards for System and Application Security as they pertain to Access Controls, System Administration and Engineering, Change Control and Configuration Management, Patch Management, Malicious Code, Monitoring and Reporting, and System Backups.
- c. **Access Controls**
Describe standards for Hiring, Termination, and Transfer of staff and how it relates to user account administration. Include a description of the process used to approve system access requests based on a need-to-know and describe how “least-privilege” is achieved in the environment.
- d. **Change Control and Configuration Management**
Describe the components of Change Control and describe the integration of the Cyber Security Program as it relates to Change Control. Describe the minimum standards for configuration management as it relates to System, Network and Application engineering.

TITLE:	CYBER SECURITY PLANNING		
POLICY #:	P-CCSP-001	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.

- e. **Physical Security**
Describe the requirements for physically securing the Agency's Sensitive Areas.
- f. **Data Handling and Disposal**
Describe the procedures used to achieve the goals of the Colorado Cyber Security Plan (CCSP) Data Handling and Disposal Policy.
- g. **Personnel Security**
Describe the process for and frequency of performing background checks on IT and Security staff
- h. **Acceptable Use**
Identify the required elements of the Agency's Acceptable Use Policy and the responsibilities for ensuring all users have received and acknowledged it.
- i. **Online Privacy**
Include the Agency's Online Privacy Notice

V. **Incident Warning, Advisory, and Response**

- a. **Cyber Security Warnings and Advisories**
Describe the process for evaluating both Vendor and Information Security Operations Center -issued Cyber Security Warnings, Patch Announcements, and Security Advisories and describe the standard for recording the response, including time frame for response, acceptable responses, and responsibilities for evaluating the Warning or Advisory.
- b. **Cyber Security Incident Response Plan Summary**
Provide a summary of the Agency's Incident Response Plan, including naming the individual(s) who lead the team.

VI. **Training and Awareness**

- a. **Methodology**
*Describe the methods for delivering Initial and Refresher Training to staff. Describe any differing levels of Cyber Security Training that are provided to individuals holding specific job responsibilities (end user, system administrator, security administrator, and managers), if applicable.
Describe methods of providing periodic security awareness notices to Agency staff, and the responsibilities for issuing these notices.*
- b. **Frequency**
Identify the required frequency for Refresher Training and Security Awareness Notices.
- c. **Content Updates**
Identify the role or individual responsible for providing updated training content and awareness notices.

TITLE:	CYBER SECURITY PLANNING		
POLICY #:	P-CCSP-001	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



- VII. Self-Assessment
Describe the required elements of the Cyber Security Self-Assessment Process, the roles and responsibilities in carrying out the Self-Assessment, and the integration of the Self-Assessment results into a program improvement process.

- VIII. Metrics and Reporting
Describe the types of metrics that are being collected by the Agency Cyber Security Program and how they are being used to evaluate the effectiveness of the Program.

- IX. Plan Approval and Maintenance
Identify the frequency of the ACSP updates and the roles that are responsible for making and approving the updates. The Agency Executive Director and the Agency CIO are required approval authorities for the ACSP.

ACSP Approval Process

Each Agency shall submit an approval package to the CISO, consisting of:

1. Cover letter requesting Plan approval
2. Agency Cyber Security Plan
3. Agency-wide Risk Assessment
4. Agency Disaster Recovery Plan Summary
5. Agency Disaster Recovery Plan test results
6. Agency Self-Assessment results
7. Agency Cyber Security Plan of Action and Milestones

Documents numbered 2 through 7, above, are not public records pursuant to Sections 24-72-202 (6) (b) (X), C.R.S. and 24-72-202 (6) (b) (XII), C.R.S. Each such document and any supporting materials shall be labeled "Confidential" and "Not a Public Record."

The cover letter is an assertion to be signed by the Executive Director that either states that the Agency is compliant with the Colorado Cyber Security Program or that the Plan of Action and Milestones contains active initiatives that will bring the Agency into compliance.

A Plan of Action and Milestones (POAM) is a high-level Plan that describes the Cyber Security initiatives under way within the Agency. This plan must include a description of the initiatives, priority, an estimated cost to the Agency to complete major project milestones, and dates of initiation and completion. This document is to be amended and maintained during the course of the year to reflect progress on the projects identified therein. The POAM may be updated by the Agency at any time throughout the year, and may be amended by the CISO at his or her discretion.

The State CISO shall review the submission to ensure it meets the requirements of the Colorado Cyber Security Plan. The CISO shall issue one of the three following responses:

1. The ACSP is approved with no changes to the submitted documents.
2. The ACSP is conditionally approved with the requirement to implement, continue, or complete the initiatives in the Agency Plan of Action and Milestones. This response

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:	CYBER SECURITY PLANNING		
POLICY #:	P-CCSP-001	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



also may include the requirement to add specific initiatives to the Agency Plan of Action and Milestones as determined by the CISO.

3. The ACSP is denied approval. This response also may be accompanied by direction from the CISO to cease or alter IT operations until specific risks have been mitigated, as determined by the CISO.

References

- ISO 17799-2005
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, rev. 1, “Guide for Developing Security Plans for Federal Systems”
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-26, “Security Self-Assessment Guide for Information Technology Systems”
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, “Risk Management Guide for IT Systems”
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, “Recommended Security Controls for Federal Information Systems”
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, “Guideline for Mapping Types of Information and Information Systems to Security Categories”
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, “Guide for the Certification and Accreditation of Federal Information Systems”
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-50, “Building an Information Technology Security Awareness Program”
- Federal Information Processing Standard (FIPS) 199, “Standards for Security Categorization of Federal Information and Information Systems.
- Federal Information Processing Standard (FIPS) 200, “Minimum Security Requirements for Federal Information and Information Systems”

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.