

TITLE:	CYBER SECURITY SELF ASSESSMENT		
POLICY #:	P-CCSP-016	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



State of Colorado Cyber Security Policies

Cyber Security Self Assessment

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).

Without a regular internal examination of processes, maintaining a positive security posture cannot be assured. Routine security reviews and audits identify residual risks and vulnerabilities which need to be acknowledged and either accepted or remedied.

Authority

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

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 must perform annual recurring Cyber Security Program Self-Assessments to measure adherence to established policies.

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 SELF ASSESSMENT		
POLICY #:	P-CCSP-016	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 for any terms not specifically defined herein.

Requirements

All State Agencies shall perform annual self-assessments that address security controls identified in the Agency Cyber Security Plan, and report the results to the State CISO.

At a minimum, this self-assessment must include:

- Vulnerability assessments of the IT environment.
- Reporting of the percentage of system users that are current on Cyber Security training requirements.
- Agency policy gap analysis versus the Colorado Cyber Security Program Policies.
- A provision for the CISO to perform independent testing in addition to the Agency's Self-Assessment.

The results of the self-assessment is used to update the Agency Cyber Security Plan providing action plans to address any gaps or shortfalls. Self Assessment results may identify security vulnerabilities and are therefore exempt from the Open Records Act.

Roles and Responsibilities

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

- Ensuring the establishment of the agency's self-assessment program.
- Providing sufficient resources to execute the self-assessment program.
- Reviewing the results of the self-assessment.
- Developing plans for corrective actions.
- Delivering the results to the State CISO (on behalf of the Executive Director) in accordance with the Cyber Security Program Plan approval process.

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

- Coordinating the development of the Agency's self-assessment program.
- Coordinating the performance of the annual self assessment.
- Delivering the results to the Agency CIO.

System and Data Owners – are responsible for:

- Supporting the Agency ISO in the development of the self-assessment program.
- Supporting the execution of the self-assessment

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 SELF ASSESSMENT		
POLICY #:	P-CCSP-016	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



Guidelines

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

Internal Audit Testing Methodology

Agency ISOs are to coordinate an annual assessment of Information Technology (IT) systems. The assessment plan is to include testing risk management and operational processes and render a report to the Agency CIO and the State CISO regarding the operational effectiveness of the Agency Cyber Security Plan and information systems operations. The Agency CIO is to prepare a plan of action along with the Security Testing and Evaluation report that identifies any future projects intended to enhance the Agency Cyber Security Plan (see the Plan Approval Process in the Information Security Program Policy for details).

Vulnerability Assessments and Penetration Testing

The Agency ISOs are to supervise an independent assessment for the effectiveness of the Agency Cyber Security Plan at least once every two years. The assessment may include evaluating systems security parameters and profiles such as access controls, password strength, network privileges, system configuration, vulnerability management, security safeguard implementation, staff training, startup files and login violations. This may be performed by contracting a commercial entity or by contracting with the Information Security Operations Center (ISOC).

Any external assessment could be leveraged to serve as Security Testing and Evaluation for the Cyber Security Plan Approval Process (see Cyber Security Planning Policy, P-CCSP-001).

Additional Guidance will be published as needed and posted to the State of Colorado Cyber Security Web Site.

Training Compliance

The Agency ISO is to assess the overall Security Awareness of the Agency by calculating the percentage of Agency personnel that have completed Cyber Security Training in accordance with State and Agency standards. To augment this statistical representation, it is recommended that the Agency ISO submits a questionnaire to a sampling of the user community that can be treated as a “pop quiz” on Information Security topics drawn from the Information Security Training material.

Cyber Policy Compliance

The Agency ISO is to oversee an independent gap analysis of the Agency’s Cyber Security Plan and supporting policies against the requirements in the Colorado Cyber Security Policies.

References

- ISO 17799-2005(E), Sections 15.2 & 15.3
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-26 Security Self-Assessment Guide for Information Technology 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.