

TITLE:	SECURITY METRICS AND MEASUREMENT		
POLICY #:	P-CCSP-017	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



State of Colorado

Cyber Security Policies

Security Metrics and Measurement

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).

The State requires uniform measurements to evaluate the overall success of the Colorado Cyber Security Program. This policy defines specific metrics which are to be used to measure the effectiveness of an Agency’s Cyber Security Program and consolidated to be used as an indicator of the overall program health.

Authority

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

Policy

Agencies shall record, review, and report key indicators that provide insight into the effectiveness of the Agency Cyber Security Plan. These key indicators shall be used to prioritize process improvement initiatives designed to improve the cyber security posture of the Agency through internal review processes and via consultation with the CISO.

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:	SECURITY METRICS AND MEASUREMENT		
POLICY #:	P-CCSP-017	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.

Definitions

Security Event – is an occurrence of a system, service or network that indicates a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant

Security Incident – is a security event for which there is a significant probability of compromising operations and threatening information security. A Security Incident causes activation of the agency's Incident Response Plan

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.

Requirements

The Agency Cyber Security Program Plan must describe:

- Metrics that are be collected
- Description of how the metrics support the Agency Cyber Security Plan
- Methods and frequency for reporting and review
- Roles and Responsibilities for data collection, reporting, review, and strategic planning

At a minimum, the Agency must collect and review on a monthly basis metrics on:

- Security Incidents
- Security Events
- Changes in user account provisioning

At a minimum, metric reporting must include:

- Monthly review of metrics by the Agency Chief Information Officer (CIO).
- Quarterly review of aggregate data by the State CISO.

Responsibilities

Agency CIO – is responsible for:

- Establishing the agency's metric collection and analysis process.
- Providing sufficient resources to execute the metric collection and analysis process.

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:	SECURITY METRICS AND MEASUREMENT		
POLICY #:	P-CCSP-017	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



- Reviewing the reported metrics.
- Using the metrics to prioritize plans and budgets for agency Cyber Security activities.
- Using the metrics to update the Agency’s Cyber Security Program Plan.

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

- Coordinating the development of the agency’s metric collection and analysis process.
- Coordinating the performance of the metric collection and analysis process.
- Delivering the metrics to the Agency CIO in accordance with the agency’s Cyber Security Program Plan.

System and Data Owners – are responsible for supporting the collection of metrics in accordance with the agency’s Cyber Security Program Plan.

Guidelines

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

Meaningful Metrics

In addition to the metrics required by this policy, an Agency is to collect additional metrics that:

- Assist in monitoring compliance with policies and requirements identified in the Agency Cyber Security Plan.
- Assist in reporting the effectiveness of the Agency Cyber Security Plan.
- Support the Agency’s business goals and objectives.
- Are required by other policy, regulation, or statute.

Examples of Candidate Metrics

Patch status by host:

- Number of hosts up-to-date (within 14 days of latest vendor security patches)
- Number of hosts out-of-date (over 14 days of latest vendor security patches)
- Number of exceptions to the agency’s patch management methodology by host

Antivirus by host:

- Number of hosts with up-to-date antivirus software monthly
- Number of hosts with up-to-date antivirus software and signatures monthly
- Number of hosts with out-of-date antivirus software monthly
- Number of hosts with out-of-date antivirus software and signatures monthly
- Number of hosts without antivirus software monthly

Risk Assessment:

- Number of system-level risk assessments performed monthly
- Number of new systems monthly and their security categorization
- Number of risk assessment updates performed monthly

TITLE:	SECURITY METRICS AND MEASUREMENT		
POLICY #:	P-CCSP-017	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



References

- ISO 17799-2005(E), Section 13.1
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-55, Security Metrics 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.