

<b>TITLE:</b>	NETWORK OPERATIONS		
<b>POLICY #:</b>	P-CCSP-006	<b>EFFECTIVE DATE:</b>	DECEMBER 20, 2006
<b>SCOPE:</b>	ALL DEPARTMENTS	<b>SUPERCEDES:</b>	FIRST RELEASE



# State of Colorado Cyber Security Policies

## Network Operations

### 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).

### 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

All Agencies shall protect information assets, data and reputation while providing a secure framework for network systems operations. Network protection methods are to be deployed that provide secure network ingress and egress points to all network enclaves and administer the supporting infrastructure in a secure manner.

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.

<b>TITLE:</b>	NETWORK OPERATIONS		
<b>POLICY #:</b>	P-CCSP-006	<b>EFFECTIVE DATE:</b>	DECEMBER 20, 2006
<b>SCOPE:</b>	ALL DEPARTMENTS	<b>SUPERCEDES:</b>	FIRST RELEASE



## Definitions

**Public Facing Systems** – is a system whose purpose is to serve information directly to anonymous internet users. Systems that require access to the trusted network in order to function can be exempted on a case-by-case basis.

**Remote Access** – is the procedure for accessing systems that are within an Agency’s internal Information Technology perimeter and considered “Internal” systems.

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

Each Agency shall define, maintain, train to, exercise, and enforce security mechanisms and written procedures for network operations that include:

- Network Access Controls
  - All Agencies must provide a method for preventing unauthorized nodes from participating on the internal network enclave and must describe this method in the Agency Cyber Security Plan (ACSP).
- Perimeter Security Administration
  - All Agency enclaves must be protected at all ingress and egress points by a firewall configured to only permit the minimum services (ports and protocols to specific systems from specific locations) required for system functionality.
    - Firewall configurations must deny access to trusted networks from un-trusted networks unless specifically permitted.
    - Firewall configurations for firewalls controlling access to High Security Enclaves must deny access to trusted networks from un-trusted networks as well as to un-trusted networks from trusted networks unless specifically permitted.
  - All Agency public-facing systems must be deployed in a DMZ that controls both ingress and egress from both internal and external networks.
  - Remote Access must be secured by using a Virtual Private Network (VPN) that requires unique user authentication in accordance with the P-CCSP-008, Access Control Policy. The tunnel established by the VPN must be encrypted and authenticated to prevent interception of data while in transit. (See P-CCSP-018, Mobile Computing)
  - Where modems are used, unique user id and complex passwords in accordance with the Access Control Policy, P-CCSP-008 must be employed along with “Dial-Back” or equivalent security mechanisms.
  - Remote enclaves that communicate over networks not directly administered by the Agency must be connected to other enclaves of the same agency using a VPN.
  - Wireless network access points are to be treated as a public-facing perimeter and must be secured accordingly. (see Wireless Security Policy, P-CCSP-019)
- Network Administration

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.

<b>TITLE:</b>	NETWORK OPERATIONS		
<b>POLICY #:</b>	P-CCSP-006	<b>EFFECTIVE DATE:</b>	DECEMBER 20, 2006
<b>SCOPE:</b>	ALL DEPARTMENTS	<b>SUPERCEDES:</b>	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.

- All network equipment (routers, switches, hubs, firewalls, VPN gateways, dial-in servers, etc) must comply with the Access Control Policy, P-CCSP-008 by requiring the use of unique user ids and complex passwords or tokens for administration and all administrative sessions must be encrypted.
- Training
  - Agency staff must be trained on the contents of this policy as applicable to their job duties.
- Monitoring and Reporting
  - Agencies shall perform Fault, Configuration, Access, Performance, and Security monitoring on all network equipment that supports the infrastructure. The standards for monitoring network infrastructure must be documented in the ACSP.
  - Anomalous behavior identified on network components must be reported to the Agency Information Security Officer (ISO) as a suspected incident in accordance with the State of Colorado Incident Response Policy, P-CCSP-002 and the Colorado Cyber Security Incident Response Plan (CSIRP).
  - All Networking devices must provide logging capabilities in accordance with Systems and Applications Security Operations Policy, P-CCSP-007.
- Inventory
  - Agencies shall inventory assets providing network infrastructure services by device, IP address, and MAC address where applicable.
  - Agencies shall keep their inventory current in accordance with the CCSP Change Control Policy and make it available to the Colorado Cyber Security Incident Response Team (CCIRT).
  - Agencies shall provide notify the Information Security Operations Center (ISOC) when inventories are updated and share the updated information with the ISOC.

## Responsibilities

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

- Defining, maintaining, and enforcing written procedures for network operations.
- Supporting the implementation and maintenance of the policy requirements with appropriate budget for staff and IT resources

**Agency ISO** – is responsible for overseeing network engineering projects and ensuring the requirements in this policy are upheld.

**Agency IT Staff** – is responsible for the administration and support of the technical requirements of this policy to include reporting to the Agency CIO and ISO.

<b>TITLE:</b>	NETWORK OPERATIONS		
<b>POLICY #:</b>	P-CCSP-006	<b>EFFECTIVE DATE:</b>	DECEMBER 20, 2006
<b>SCOPE:</b>	ALL DEPARTMENTS	<b>SUPERCEDES:</b>	FIRST RELEASE



## Guidelines

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

### Network Access Controls

Access controls policies and procedures for network access are governed by Access Control Policy, P-CCSP-008. Procedures are to be developed using the following guidelines.

- Unique User Identification
- Logical Access Controls, including:
  - All Local Area Networks (LAN) are to be protected by a properly configured firewall to limit access from un-trusted network locations
  - All sensitive data is to be stored and processed on a LAN segment that is separated from end users through the use of a firewall or other access control mechanism.
  - All publicly accessible applications are to be deployed in a logical or physical DMZ, protected from the public and from the internal systems by properly configured firewalls.

### Perimeter Security Administration

Each Agency shall develop and publish Firewall Management Policy and Procedures using the following guidance.

- Firewalls are to be configured to deny all traffic from un-trusted network locations. Business justification is required to open any port or enable any service from an un-trusted network connection.
- Firewall rules are to be reviewed by the Agency Information Security Officer at least once per year.
- Each firewall must be configured to log and report rule violations to the administrator.
- All network and security devices are to be configured and hardened according to the recommendations published by the ISOC. The hardening procedures require disabling or removing all unnecessary services or functions.
- Monitoring, event logging and analysis processes and systems are to be deployed to record and analyze security events and to monitor the firewall and other security devices.

### Network Administration

An Agency defines procedures, drafts diagrams and maintains inventories including:

- Inventory critical network devices and software
- Diagrams of critical network connections that define the function, name, location, IP address and capacity of critical network and security devices, services, host systems, applications and confidential data storage.
- Vulnerability Assessment and Patch Management for Network Infrastructure devices.

These diagrams, inventories, and procedures are to be made available to the CISO's office.

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.

<b>TITLE:</b>	NETWORK OPERATIONS		
<b>POLICY #:</b>	P-CCSP-006	<b>EFFECTIVE DATE:</b>	DECEMBER 20, 2006
<b>SCOPE:</b>	ALL DEPARTMENTS	<b>SUPERCEDES:</b>	FIRST RELEASE



## Training

Network Administration staff is to be trained on each critical system prior to making changes to any system. Each network administrator is encouraged to obtain industry and vendor certification for the skills necessary for operating critical systems.

## Monitoring and Reporting

Each Agency shall establish monitoring and reporting procedures for the following functions.

- Capacity and Utilization Management of all network and security devices including firewall load.
- Security Event Logging, Analysis and Reporting

## Audit and Testing

Each Agency shall establish procedures to accomplish the following objectives:

- Internal tests to periodically verify compliance to these policies.
- Periodic external testing, including vulnerability tests and penetration tests, which are obtained from an independent third party to verify compliance to these policies and regulatory requirements. Independent external security and vulnerability assessments are to be performed at least once per year and results made available to the State CISO. Independent testing to satisfy this requirement may be accomplished by the office of cyber security. Vulnerability analysis is also conducted after any significant infrastructure or application upgrade or modification.
- Annual Disaster Recovery Tests.

## Additional Guidance

Where possible and practical, implementation of the following is encouraged.

- Services and trust extended from external networks are to be limited to the minimum necessary to accomplish the task requiring the interface.
- Configuration changes (i.e., new administrator, enabling new service, loading new operating system) must be documented as part of the Agency Configuration Management / Change Control Policy and procedures (see Change Control Policy, P-CCSP-009).
- Administrative functions are to be performed directly on the console or inside an encrypted link [e.g. Secure Shell (SSH), or Data Encryption Standard (DES) tunnel].
- Questionable or unusual activities must be immediately reported to the department Information Security Officer.
- Installation of new equipment requires all vendor-supplied default settings be changed prior to deployment as outlined in the device hardening guidelines (i.e. passwords, community strings, unnecessary accounts or services, etc.)

<b>TITLE:</b>	NETWORK OPERATIONS		
<b>POLICY #:</b>	P-CCSP-006	<b>EFFECTIVE DATE:</b>	DECEMBER 20, 2006
<b>SCOPE:</b>	ALL DEPARTMENTS	<b>SUPERCEDES:</b>	FIRST RELEASE



## References

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-44, “Guidelines on Securing Public Web Servers”
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-41, “Guidelines on Firewalls and Firewall Policy”
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, “Recommended Security Controls for Federal Information Systems”
- CCSP Access Control Policy, P-CCSP-008
- Cyber Security Program Policy , P-CCSP-001

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.