

<b>TITLE:</b>	WIRELESS SECURITY		
<b>POLICY #:</b>	P-CCSP-019	<b>EFFECTIVE DATE:</b>	DECEMBER 20, 2006
<b>SCOPE:</b>	ALL DEPARTMENTS	<b>SUPERCEDES:</b>	FIRST RELEASE



# State of Colorado Cyber Security Policies

## Wireless Security

### 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.

### 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 the use of wireless technology.

### 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 Planning Policy Glossary for any terms not specifically defined herein.

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>	WIRELESS SECURITY		
<b>POLICY #:</b>	P-CCSP-019	<b>EFFECTIVE DATE:</b>	DECEMBER 20, 2006
<b>SCOPE:</b>	ALL DEPARTMENTS	<b>SUPERCEDES:</b>	FIRST RELEASE



## Requirements

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

### Perimeter Protection Controls and Device Security

Due to the fact that wireless access points allow anonymous access to the network they reside upon, all access points are to be controlled as a network perimeter as detailed in Network Operations Policy, P-CCSP-006). In addition, the following controls must be implemented.

- All agencies are to create an inventory of their wireless equipment and maintain that inventory as network changes occur.
- During installation and before connection to a State network all default passwords and Service Set IDs (SSID) are to be changed on wireless access points and on wireless devices (where applicable).
- Wireless access points are to be configured to not broadcast their SSID unless they are intended for public access.
- Wireless access points intended for providing connectivity to end-user systems are to be configured to use 128bit Wireless Encryption Protocol (WEP) encryption at a minimum. It is highly recommended to implement Wi-Fi Protected Access (WPA) with Pre-shared Key (PSK) on devices with this capability and to upgrade systems that do not.
- If the wireless access point has a factory reset button, then physical access to the device is to be limited to system administrators only.
- If wireless technology is used for point-to-point connectivity the wireless access points on either end of the connection are to be connected to a firewall that limits access to only traffic from the other antenna and the network behind it.

### Encryption Requirements

- All multi-user access points are to be configured to require, at a minimum, 128 bit WEP encryption.
- Point-to-Point wireless links are to be protected using an IPSec encrypted tunnel between firewalls on either end of the wireless link.

## Responsibilities

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

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

**Agency Information Security Officer (ISO)** – is responsible for overseeing wireless projects to ensure the requirements in this policy are upheld.

**Agency IT Staff** – is responsible for administering and supporting the technical requirements of this policy, including reporting to the Agency CIO and ISO.

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>	WIRELESS SECURITY		
<b>POLICY #:</b>	P-CCSP-019	<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.

- Perimeter Protection Controls and Device Security
  - All access points used by the State are to support logging and all logs should be forwarded to a central log server.
  - Repeated failed attempts to access the wireless network is to be reported to the agency ISO and/or the Information Security Operations Center (ISOC).
  - Intrusion detection systems are to be placed on subnets that have wireless access present.
  - When placing wireless access points in a building it is recommended that they are placed as far from the exterior of the building as practicable.
  - Users are not to be given access to the wireless network unless specifically authorized.
- Encryption Requirements
  - Wi-Fi Protected Access (WPA) with Temporal Key Integrity Protocol (TKIP) or Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) using IEEE 802.1X or Pre-shared key (PSK) authentication is the preferred security configuration for wireless access points.
  - Encryption keys are to be treated as passwords and changed and controlled in accordance with Access Control Policy, P-CCSP-008.

## References

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-77 “Guide to IPsec VPNs”
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-48 “Wireless Network Security: 802.11, Bluetooth, and Handheld Devices”
- 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.