

TITLE:	DATA HANDLING AND DISPOSAL		
POLICY #:	P-CCSP-011	EFFECTIVE DATE:	MARCH 4 th , 2007
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	SECOND RELEASE



State of Colorado Cyber Security Policies

Data Handling and Disposal

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 majority of data used to deliver services to the citizens of Colorado is subject to public disclosure as a public record. However, this policy provides guidelines to protect data that contains information that has been excluded from public records. Data that has been excluded from public records includes data subject to protection under federal regulations.

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).

C.R.S. 24-72-204 for public record exemption.

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:	DATA HANDLING AND DISPOSAL		
POLICY #:	P-CCSP-011	EFFECTIVE DATE:	MARCH 4 th , 2007
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	SECOND 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.

Policy

All Agencies shall develop and maintain procedures to protect non-public information while it is being collected, processed, stored or transported in electronic form. Agencies shall provide resources to perform these actions and train departmental staff on the procedures.

In addition to protecting non-public information, agencies shall comply with all federal and State privacy and data security regulations as well as contractual obligations to protect information.

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.

Requirements

All Public Agencies must establish and enforce policies and procedures that address:

- Methods of storage, transmission, and destruction when in electronic format
- Methods of storage when stored on portable computing systems
- Methods of storage when stored on non-State systems (e.g., vendors, contractors)

All public agencies must define data types and categorize them into the following four levels, according to agency impact:

- **Unrestricted** – information that would have no measurable impact on the agency in the event of a breach of confidentiality, loss of integrity, or lack of availability.
- **Level 1** – information that would have little impact on the agency in the event of a breach of confidentiality, loss of integrity, or lack of availability.
- **Level 2** – information that would have significant financial or operational burden on an agency in the event of a breach of confidentiality, loss of integrity, or lack of availability.
- **Level 3** – information that is required by federal, State, or local law to be protected, or in the event of a breach of confidentiality, loss of integrity, or lack of availability would have serious impact to the agency up to and including physical harm to individuals, or that which would cause significant hardship to the agency, state, commercial entities that have entrusted this data to the agency.

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:	DATA HANDLING AND DISPOSAL		
POLICY #:	P-CCSP-011	EFFECTIVE DATE:	MARCH 4 th , 2007
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	SECOND RELEASE



Disposal: All Public Agencies must implement approved methods of destruction for each data type. These methods are outlined in the following minimum requirements table:

Data Type		Electronic Deletion / Destruction
Unrestricted	NS	Standard file deletion
Level 1		Standard file deletion
Level 2	SENSITIVE	Data destruction is to be accomplished in accordance with Office of Information Technology (OIT) Data Destruction Policy.
Level 3		Data destruction is to be accomplished in accordance with OIT Data Destruction Policy. A record of disposal shall be maintained.

Where required by law, regardless of the sensitivity of the data, a record of disposal is to be maintained by the agency. A record of disposal must contain the name of the individual disposing of the data, the method used to dispose of the data, identifying qualities of the data (such as the serial number of the media on which it was stored, if applicable), and the date of disposal.

Storage: All Public Agencies must implement approved methods of storage for each data type. Electronic destruction for is only required when disposing or recycling / repurposing the media. These methods are outlined in the following minimum requirements table:

Data Type		Electronic Storage
Unrestricted	NS	No Requirements
Level 1		No Requirements
Level 2	SENSITIVE	Encrypted when stored on removable media or on portable systems Encrypted when stored on systems managed by a vendor performing services for the state.
Level 3		Encrypted when stored on state systems, where feasible. Encrypted when stored on removable media or on portable systems. Encrypted when stored on systems managed by a vendor performing services for the state. Enable logging to identify access to confidential data and securely-stored logs in accordance with the System And Applications Security Policy, P-CCSP-007.

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:	DATA HANDLING AND DISPOSAL		
POLICY #:	P-CCSP-011	EFFECTIVE DATE:	MARCH 4 th , 2007
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	SECOND RELEASE



Transmission and Transportation: All Public Agencies must implement approved methods of transmission for each data type. These methods are outlined in the following minimum requirements table:

Data Type		Electronic Transmission
Unrestricted	NS	No requirement
Level 1		No requirement
Level 2	SENSITIVE	Data must only be transported or transmitted when protected by an approved encryption solution. When data is stored on electronic media or a mobile computing device, the data must be encrypted at all times during physical transport). Transmission by unencrypted e-mail is prohibited.
Level 3		Data must only be transported or transmitted when protected by an approved encryption solution. When data is stored on electronic media or a mobile computing device, the data must be encrypted at all times during physical transport). Transmission by unencrypted e-mail is prohibited.

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.

Responsibilities

Agency Executive Director – is responsible for ensuring the development of and approval of a sensitivity classification scheme for data types.

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

- Working with system owners to identify data types for classification.
- Ensuring that all personnel are trained in media handling procedures specific to their department;
- Ensuring IT staff have the appropriate resources to execute this policy.

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

- Maintaining a list of media types with assigned classification.
- Maintaining an inventory of systems and their associated data classification.
- Assisting Agency staff in carrying out this policy.

TITLE:	DATA HANDLING AND DISPOSAL		
POLICY #:	P-CCSP-011	EFFECTIVE DATE:	MARCH 4 th , 2007
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	SECOND RELEASE



- Reporting any violations to this policy to the State CISO in the event the disclosure constitutes an incident.

Guidelines

Agencies are to consider implementing the following control guidelines when handling and disposing of sensitive information.

Media Inventory

The Agency Information Security Officer (ISO) is to maintain a list of storage media with assigned classification. This data classification scheme and the inventory of all agency data by type is a critical element in the Agency completing a comprehensive risk assessment. The inventory is to be updated at least once per year as a part of the risk assessment update. Data classification is to be included in staff orientation and training.

Handling of Physical Media

Sensitive information may be stored on media such as magnetic and optical disks, backup tapes, and other electronic media. Media containing sensitive information is to be appropriately labeled and protected according to its sensitivity as defined in the media classification inventory.

All electronic media is to be labeled prior to storage or transmission outside the State. Electronic files are to be marked with a label identifying the data type. For systems that provide a dynamic view of data elements that meet the criteria for sensitive information, the Interface is to contain this marking, as well as printed output. Exceptions to this guideline may be addressed in End-User Training.

Information Retention

With the passage of time, sensitive information which was initially collected and retained for a legitimate agency purpose may no longer be necessary to retain for any business purpose. The Agency should defer to policy endorsed by its executive director or the Colorado State Archives for specific direction.

Information Disposal

When disposing of electronic media that previously contained sensitive information, the Agency CIO is responsible for ensuring that all media is electronically disposed of in accordance with the Colorado Data Destruction and Computers and Other Electronic Media End-Of-Life policy.

Clean Desk Policy

Employees, when possible, are to secure media containing sensitive information by maintaining a clean desk and/or locking media in a secure room when they are out of the office. Media security may be achieved through locking the door to a private office or locking media in a cabinet or drawer.

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:	DATA HANDLING AND DISPOSAL		
POLICY #:	P-CCSP-011	EFFECTIVE DATE:	MARCH 4 th , 2007
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	SECOND RELEASE



References

ISO 17799-2005, Code of Practice for Information Security, Section 7 Asset 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.