

<b>TITLE:</b>	DISASTER RECOVERY		
<b>POLICY #:</b>	P-CSPP-004	<b>EFFECTIVE DATE:</b>	MARCH 4 <sup>th</sup> , 2006
<b>SCOPE:</b>	ALL DEPARTMENTS	<b>SUPERCEDES:</b>	SECOND RELEASE



# State of Colorado

## Cyber Security Policies

### Disaster Recovery

#### 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 Public 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 Public Agencies achieve the objective of this Policy.

For the purposes of this document, a “Public Agency” includes organizations as defined in C.R.S. 24-37.5-102(5).

#### Policy

It is the policy of the State of Colorado that all State Public Agencies and associated departments prepare and test Disaster Recovery Plans that will be maintained and used in the event of a disaster.

#### Authority

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

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>	DISASTER RECOVERY		
<b>POLICY #:</b>	P-CSPP-004	<b>EFFECTIVE DATE:</b>	MARCH 4 <sup>th</sup> , 2006
<b>SCOPE:</b>	ALL DEPARTMENTS	<b>SUPERCEDES:</b>	SECOND RELEASE



## Scope

This policy document applies to every State Public 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

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.

## Roles and Responsibilities

**Agency Executive Director** – is responsible for appropriate funding to the IT department sufficient to support Disaster Recovery planning and testing needs.

**CISO** – is responsible for review and approval of Public Agency Disaster Recovery Plans and test results as part of the Cyber Security Program Plan approval process.

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

- Leading the development of the Public Agency Disaster Recovery Plan.
- Coordinating testing of the Disaster Recovery Plan

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

- Monitoring the effectiveness of the disaster recovery planning and preparation process.
- Ensuring required security controls are implemented during Disaster Recovery operations.

**Agency IT Staff** – is responsible for:

- Completing disaster recovery training.
- Participating as required in disaster recovery testing.

## Requirements

To ensure adherence to best practices and industry standards, this policy requires that all Public Agencies develop a Disaster Recovery Plan and comply with the following:

### Development of the Disaster Recovery Plan

IT Disaster Recovery Plans are to be developed and designed to reduce the impact of a major disruption on key business functions and processes. The Disaster Recovery Plans must address requirements for alternative processing and recovery capability of all critical IT services. Disaster Recovery Plans must also include usage guidelines, roles and responsibilities, procedures, communication processes, and the testing approach. The systems, applications, and resources identified as the most critical should be the focus in the IT Disaster Recovery Plan. This will establish the priorities in recovery situations and to keep costs at an acceptable level while complying with regulatory and contractual requirements. Response and recovery requirements for different timeframes (e.g., within

<b>TITLE:</b>	DISASTER RECOVERY		
<b>POLICY #:</b>	P-CSPP-004	<b>EFFECTIVE DATE:</b>	MARCH 4 <sup>th</sup> , 2006
<b>SCOPE:</b>	ALL DEPARTMENTS	<b>SUPERCEDES:</b>	SECOND RELEASE



the first 24 hours, the next 48 hours, fourth through seventh days, and extended disaster period) must be addressed in the Disaster Recovery Plan if applicable to the Public Agency's IT disaster recovery scenario.

Maintenance of the Disaster Recovery Plan

Disaster Recovery Plan maintenance procedures will be defined to ensure that that the Plan is kept up to date with respect to dynamic changes, such as personnel changes, new system deployment, documentation updates, and to ensure it continually reflects business requirements. The Disaster Recovery Plan shall also contain instruction to notify stakeholders of changes to the plan.

Testing of the Disaster Recovery Plan

IT Disaster Recovery Plans are to be tested on a regular basis to ensure that IT systems can be effectively recovered and shortcomings can be addressed. Disaster Recovery Plan testing must identify testing procedures and contain instruction how the public agency will approve updates to the Plan based on test results.

Training on the Disaster Recovery Plan

All concerned parties are to receive regular training sessions regarding the procedures and their roles and responsibilities in case of an incident or disaster. The Disaster Recovery Plan must contain instruction on how training is enhanced or distributed in the event of new Plan requirements, roles, responsibilities, or communication processes.

Distribution of the Disaster Recovery Plan

A defined and managed distribution strategy must be outlined in the Disaster Recovery Plan to ensure that the Plans are properly and securely distributed and available to appropriately authorized interested parties when and where needed. This distribution strategy must take into account all disaster scenarios that the Plan is intended to address.

IT Services Recovery and Resumption

The Disaster Recovery Plan must be supported with step-by-step instructions for recovery and resumption of services. This may include activation of backup sites, initiation of alternative processing, customer and stakeholder communication, resumption procedures, etc.

Offsite Backup Storage

All backup media, documentation and other IT resources necessary to recover or resume IT processing must be stored off-site. Backup procedures and rotation schemes must be adequate to provide the necessary data for recovery while minimizing data loss. IT management should ensure that offsite arrangements are periodically assessed, at least annually, for content, environmental protection and security. Backup media and the hardware used to restore from backup must be tested as part of the Disaster Recovery Plan testing strategy.

Post-Resumption Review

A post-resumption review must occur after successful resumption of the IT functions following a disaster. The purpose of this review is to assess the adequacy of the Disaster Recover Plan and procedures, and to subsequently update the Plan accordingly.

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>	DISASTER RECOVERY		
<b>POLICY #:</b>	P-CSPP-004	<b>EFFECTIVE DATE:</b>	MARCH 4 <sup>th</sup> , 2006
<b>SCOPE:</b>	ALL DEPARTMENTS	<b>SUPERCEDES:</b>	SECOND RELEASE



## Guidelines

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

### Disaster Recovery Plan Development

Public Agencies should perform a Business Impact Assessment to identify IT systems that would have the greatest negative impact to the Public Agency in the event of a disaster. Such systems should be used to prioritize the recovery scope and schedules.

A Threat and Vulnerability Analysis should be conducted to identify the most probable disaster scenarios. The most probable scenarios should be used to guide the development of the Disaster Recovery Plan strategy.

### Continuity Planning

Public Agencies should address business continuity in a formal Business Continuity Plan (BCP). Depending on the size and complexity of the organization, it is feasible to include it in the Disaster Recovery Plan, but it is advised to maintain it in a separate but closely related document.

### Contact Information

The Disaster Recovery Plan should address roles, responsibilities, and identify both primary and secondary individuals with contact information, and activities associated for both primary and secondary individuals in executing the disaster recovery plan.

The Disaster Recovery Plan should be updated quarterly to address changes in systems and organizations.

### Disaster Recovery Plan Training

Public Agencies should keep auditable records of disaster recovery training and validate that the team members have received training prior to each disaster recovery test (or more frequently). Training should be delivered to all individuals that are assigned roles in the Disaster Recovery Plan.

End-user training should address expectations of the user in the event of a disaster and should be delivered on initiation of employment with refresher training administered periodically thereafter.

### Enhanced Disaster Recovery Plan Testing

Testing of the Disaster Recovery Plan is occasionally expanded to include full-scale execution for critical systems. The depth and rigor of testing is balanced against the potential impacts to on-going operations. At a minimum, operational testing of the Disaster Recovery Plan is performed for critical systems.

### Recovery and Resumption

#### Alternate Storage, Processing, and Operations

An alternate processing site should be geographically separated from the primary processing site so as not to be susceptible to the same hazards. A rule of thumb to be used is to locate the alternate processing site 200 to 300 miles away from the primary processing facility.

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>	DISASTER RECOVERY		
<b>POLICY #:</b>	P-CSPP-004	<b>EFFECTIVE DATE:</b>	MARCH 4 <sup>th</sup> , 2006
<b>SCOPE:</b>	ALL DEPARTMENTS	<b>SUPERCEDES:</b>	SECOND RELEASE



The alternate processing site should be configured to facilitate timely and effective recovery operations and maintain the appropriate security controls for critical systems.

A Public Agency identifying an alternate processing site should initiate the necessary agreements to permit the resumption of operations for critical functions within a specifically defined period of time when the primary processing capabilities are unavailable.

Equipment and supplies required to resume operations should be available at the alternate site or there should be contracts in place to support immediate delivery to the site.

The alternate processing site should be fully configured to support the minimum required operational capability and be ready to use as the operational site with little or no notice and no intervention by Public Agency IT staff.

The alternate processing site may optionally be used as the business operations alternate site to reduce cost and impact to the public agency. In this configuration, however, care should be taken to uphold reasonable physical security controls.

#### Telecommunications Support

The Public Agency should identify primary and alternate telecommunications services and initiate necessary agreements to permit the resumption of system operations for critical functions when the primary telecommunications capabilities are unavailable.

Ubiquitous use of cellular phones may help defray some of the costs involved in setting up voice telecommunications, but care should be taken to ensure reception at the alternate facility is adequate for operational needs.

### **Offsite System Backups**

The Public Agency should conduct backups of user-level and system-level information and protect backup information from loss, theft, or modification while in transit and at the backup media offsite storage location. The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) is to be consistent with the public agency's recovery time objectives.

At a minimum, the Public Agency backup plan includes:

- Daily incremental backups of all critical systems
- Weekly full backups of all critical systems and off-premise media rotation.
- Monthly full backups and off-premise storage for disaster recovery purposes.
- Labeling of backup media to indicate its data classification level.

The public agency should test backup information frequently to ensure media reliability and information integrity.

### **Post-resumption**

Lessons learned workshops should be held immediately following recovery and the results of this lessons learned should add to the public agency's Plan of Action and Milestones (POA&M).

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>	DISASTER RECOVERY		
<b>POLICY #:</b>	P-CSPP-004	<b>EFFECTIVE DATE:</b>	MARCH 4 <sup>th</sup> , 2006
<b>SCOPE:</b>	ALL DEPARTMENTS	<b>SUPERCEDES:</b>	SECOND RELEASE



## References

- ISO 17799-2005 Section 10 Business Continuity/Disaster Recovery
- National Institute of Standards and Technology (NIST) Special Publication (SP)-800-34, “Contingency Planning Guide for Information Technology Systems”
- IMC Disaster Recover Policy Statement

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.