



State of Illinois

Department of Central Management Services

**MIDRANGE BACKUP
(TSM Shared Services)
POLICY**

Effective December 1, 2007

State of Illinois
Department of Central Management Services
Bureau of Communication and Computer Services

MIDRANGE BACKUP POLICY

Effective December 1, 2007
Version 1.0

APPROVAL SHEET

CMS/BCCS Deputy Director:



Doug Kasamis

Date: 11/29/07

CMS/BCCS Deputy General Counsel:



Dominic Stebeler

Date: 11/29/07

CMS/BCCS Chief Security Officer:



Rafael Diaz

Date: 11/29/07

Please Return to: CMS/BCCS
Chief Security Office
120 W. Jefferson
Springfield, IL 62702

Thank You.

Illinois Department of Central Management Services
MIDRANGE BACKUP POLICY

TABLE OF CONTENTS

POLICY STATEMENT

PURPOSE

SCOPE

DEFINITIONS

RESPONSIBILITY

POLICY

Illinois Department of Central Management Services
MIDRANGE BACKUP POLICY

POLICY STATEMENT

This document defines the backup policy for CMS/BCCS supported computer systems maintained by the consolidated Tivoli Storage Manager (TSM) backup systems.

PURPOSE

This policy is designed to prevent the loss of State of Illinois System and Business Application data in the event of an equipment failure or destruction.

SCOPE

This policy applies to all midrange equipment, including the data housed on that equipment, owned and operated by CMS/BCCS, and maintained by the consolidated Tivoli Storage Manager backup systems. Consolidated Agencies are expected to follow this policy for data they continue to maintain. Non Consolidated Agencies are advised to follow this policy as a best practice.

DEFINITIONS

The following terms are used in this policy. Additional terms may be used and can be found in the BCCS Terminology Glossary document located at the BCCS Web site bccs.illinois.gov.

1. Backup - The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.
2. Archive - The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.
3. Consolidated Agency - Agency whose IT infrastructure and staff were consolidated into CMS as part of the IT rationalization efforts that began in FY 2004.

RESPONSIBILITY

CMS/BCCS Staff - It is the responsibility of BCCS staff to familiarize themselves with the backup policy and to follow the policy and corresponding procedures.

Consolidated Agency IT Staff - It is the responsibility of the Consolidated Agency IT staff to inform BCCS staff, in writing, of special backup requirements outside of this policy. Those exceptions could include frequency and/or timeframe deviations from the policy.

CMS / BCCS is not responsible for the backup of data stored on personal computers (PC) or laptops (LT).

POLICY

1. All data files (i.e., word processing, database, spreadsheets) and email are eligible for backup with the exception of the files listed in the backup software exclude list. Each exclude list is tailored for the system being backed up.

Illinois Department of Central Management Services
MIDRANGE BACKUP POLICY

2. The initial backup for each TSM client (agency server) is a full backup.
3. Daily incremental backups are performed after the initial full backup. Only data files that have changed since the previous backup will be backed up.
4. Up to 15 backup versions of each data file are stored on the TSM server.
5. The most recent backup version of a data file on the TSM server is stored in an active state. For all data files that exist on the TSM client there will always be one active backup version of the file stored on the TSM server.
6. Older versions of data file backups will be stored in an inactive state on the TSM server. Data file backups that have been in an inactive state on the TSM server for more than 45 days will be deleted.
7. If a data file is deleted from a TSM client, 2 of the 15 possible backup versions of this file will be retained on the TSM server. The other 13 versions are removed from the TSM server. Of the 2 backup versions retained, the oldest version will be deleted from the TSM server in 45 days. The last (only) remaining backup version of this file will be kept on the TSM server for 60 days.
8. Archives of data files are performed once a month (dates will vary to avoid scheduling conflicts) on all servers and retained for a year. The archive tapes are shipped to the regional vault on Monday, Wednesday and Friday and brought back as needed for restores.
9. Backups of email are performed daily and retained for 365 days. The email tapes are shipped to the regional vault on Monday, Wednesday and Friday and brought back as needed for restores.
10. Offsite tape copies of all backup data are created daily for use in the event of a disaster. The offsite tapes are shipped to the regional vault on Monday, Wednesday and Friday and are returned from the off-site vaulting facility as needed.
11. If a file or directory is modified or open during the backup cycle, it is not backed up.
12. Existing legacy (pre-consolidation) systems backup policies, where documented, will be followed as documented until they are converted to the shared services TSM backup system. If no documentation exists, existing standard business practices will be followed.
13. Policy exceptions due to legal or procedural requirements will be reviewed and approved by the CMS BCCS Deputy Director, the CMS BCCS Deputy General Counsel, and the CMS BCCS Chief Security Officer.

Illinois Department of Central Management Services
MIDRANGE BACKUP POLICY

REVISION HISTORY

Created: June 1, 2007
Revised: October 16, 2007
Reviewed: October 16, 2007
Effective: December 1, 2007