

ENT-NET-010

STATEWIDE INFORMATION SYSTEMS POLICY

LAN Backup And Archiving Plan

Approved

Office of the Chief Information Officer

Department of Administration
Information Technology Services Division
PO Box 200113
Helena, MT 59620-0113
Tel: (406) 444-2700
FAX: (406) 444-2701

March 1998



Brian Schweitzer
Governor

State of Montana

DEPARTMENT OF ADMINISTRATION

Janet R. Kelly, Director

CHIEF INFORMATION OFFICER

Richard B. Clark

APPROVED STATEWIDE POLICY: LAN BACKUP AND ARCHIVING PLAN

EFFECTIVE DATE: MARCH 11, 1998

APPROVED: MARCH 11, 1998

I. Purpose

The Department of Administration's Information Technology Services Division (ITSD) is responsible for providing security for the Montana state network. This **LAN Backup And Archiving Plan Policy** (Policy) identifies the responsibilities for backing up and archiving data.

II. Authority

Pursuant to the Montana Information Technology Act (MITA) (Title 2, Chapter 17, Part 5 of the Montana Code Annotated (MCA), it is the policy of the state that information technology be used to improve the quality of life of Montana citizens, and that such improvement is to be realized by protecting individual privacy and the privacy of the information contained within the state's information technology systems. [§2-17-505\(1\) MCA](#).

It is also the policy of the state that the development of information technology resources be conducted in an organized, deliberative, and cost-effective manner, which necessitates the development of statewide information technology policies, standards, procedures, and guidelines applicable to all state agencies and others using the state network. It is also anticipated that State information technology systems will be developed in cooperation with the federal government and local governments with the objective of providing seamless access to information and services to the greatest degree possible. [§2-17-505\(2\) MCA](#).

III. Roles And Responsibilities

A. Department of Administration

Under MITA, the Department of Administration (DOA) is responsible for carrying out the planning and program responsibilities for information technology for state government (except the national guard), including for establishing and enforcing a state strategic information technology plan and establishing and enforcing statewide information technology policies and standards. DOA is responsible for implementing MITA and all other laws for the use of information technology in state government. The director of DOA has appointed the chief information officer to assist in carrying out the department's information technology duties. [§2-17-512 MCA](#).

B. Department Heads

Each department head is responsible for ensuring an adequate level of security for all data within their department. [§2-15-114 MCA](#).

IV. Applicability

This Policy is applicable to agencies, staff and all others, including outsourced third-parties (such as contractors, or other service providers), which have access to, or use or manage information assets subject to the policy and standard provisions of [§2-17-534, MCA](#). This Policy shall be communicated to staff and others who have access to or manage information, and information systems and assets.

V. Scope

This Policy encompasses information and information systems for which agencies have administrative responsibility, including information and systems managed or hosted by third-parties on agencies' behalf.

This Policy may conflict with other information system policies currently in effect. Where conflicts exist, the more restrictive policy governs. The development of future policies or standards will specifically identify and retire any superseded portions of current policies or standards.

VI. Requirements

This policy refers to local area networks which includes file servers and workstations.

For the purposes of this policy, the following definitions apply:

- Backup** A disk or tape on which important data is duplicated for the purpose of safety. Should the original stored information become corrupt or lost, the information can be retrieved from the backup. A backup allows for recovery of data in the case of a disaster.
- Electronic Archiving** The act of storing electronic files for future retrieval. If an electronic document is ever needed in the future, it should be archived. Only select documents should be archived.
- Archives** Those records that have been determined to have sufficient historical or other value to warrant their permanent preservation and that have been transferred to the State Archive's custody.

Each agency must have a written backup plan including a backup schedule, backup process and a list of mission critical applications. Agencies should consider their current electronic archiving process (the storing of files for future retrieval, not the process of sending documents to the State Archives) while developing their backup plan. Agencies cannot use the backup process as an electronic archiving method; a separate electronic archiving process and plan must be developed. The backup plan must be reviewed annually and periodically tested by the agency network administrator. Each agency must maintain a notification list of designated staff to be contacted in an emergency. A copy of this list must be kept in a secure location, such as with off-site backups, and be readily accessible in case of an emergency.

At a minimum, modified data on file servers must be backed up at the end of each work day and a full system backup must be performed at least once a week. Mission critical data should be backed up, regardless of where it resides. On a monthly basis at least one full backup must be stored off-site.

Agencies must retain backup tapes for no longer than thirty (30) days unless this retention schedule is extended by an agency head to address a compelling business need for the agency. The backup tapes must be erased and reused, or destroyed, after thirty (30) days.

Weekly backups of the NetWare Directory Structure (NDS) will be completed by the Information Technology Services Division, Department of Administration. Network Administrators must contact the [ITSD Service Desk](#) for NDS restorations.

A. Background - History On The Creation Of Or Changes To This Policy

This policy was originally created by the NetWare Managers Group Policy Committee. It was then modified to reflect concerns of document and email retention and was reviewed by an ad hoc committee created by Lois Menzies, Director of the Department of Administration. The Information Technology Advisory Council reviewed and approved this policy.

B. Guidelines - Recommendations, Not Requirements

It is recommended agencies maintain a list of hardware specifications for all critical systems to insure appropriate replacement hardware can be provided in case of a disaster. Network administrators should be trained in the use of current backup hardware, software and policies. Agencies should insure users are trained in proper workstation backup procedures.

It is also recommended agencies maintain a set of diskettes containing an emergency recovery configuration and backup software both on-site and off-site. Agencies should test the viability of these diskettes to recover the system and load the backup software in order to perform a full system restore.

A consideration for an agency's electronic archiving plan is to designate certain directories or drives for electronic archiving. These directories or drives should not contain email or documents which are considered temporary. Another consideration for an agency's electronic archiving plan is to include a migration plan for transferring data from one media to another as technology changes.

References - Laws, rules, standard operating procedures and applicable policies

VII. Change Control and Exceptions

Policy changes or exceptions are governed by the [Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards](#). Requests for a review or change to this instrument are made by submitting an [Action Request](#) form (at http://itsd.mt.gov/content/policy/policies/administration/action_request.doc). Requests for exceptions are made by submitting an [Exception Request](#) form (at

http://itsd.mt.gov/content/policy/policies/administration/exception_request.doc). Changes to policies and standards will be prioritized and acted upon based on impact and need.

VIII. Closing

Direct questions or comments about this instrument to the State of Montana Chief Information Officer at [ITSD Service Desk](mailto:ITSD_Service_Desk) (at <http://servicedesk.mt.gov/ess.do>), or:

PO Box 200113
Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

IX. References

A. Legislation

- [2-17-505\(1\)](#) – Policy
- [2-17-514\(1\)](#) – Enforcement
- [§2-17-505\(2\), MCA](#)
- [2-17-512, MCA](#)
- [2-17-534, MCA](#)
- [2-15-114, MCA](#)

B. Policies, Directives, Regulations, Rules, Procedures, Memoranda

- MOM 3-0130 Discipline
- ARM 2.13.101 - 2.13.107 - Regulation of Communication Facilities
- ARM 2.12.206 Establishing Policies, Standards, Procedures and Guidelines.
- [Statewide Policy: Establishing and Implementing Statewide Information Technology Policies and Standards](#)
- [Statewide Procedure: Establishing and Implementing Statewide Information Technology Policies and Standards](#)

C. Standards, Guidelines

X. Administrative Use

Product ID: ENT-NET-010
Proponent: Chief Information Officer
Publisher: Office of the Chief Information Officer
Published Date: March 1998
Version Date: 6/8/2010
Custodian: Policy Manager
Approved Date: March 11, 1998
Effective Date: March 11, 1998
RIM Class: Record
Disposition Instructions: Retain for Record
Change & Review: [ITSD Service Desk](http://servicedesk.mt.gov/ess.do) (at <http://servicedesk.mt.gov/ess.do>)
Contact:
Review: Event Review: Any event affecting this instrument may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date: April 7, 2014
Last Review/Revision: May 4, 2009
Changes: July 11, 2008 – Non-material changes made:

- Standardize instrument format and common components.
- Changed to reflect next review date.

April 7, 2009 – Non-material changes made:

- Corrected broken URLs
- Applied new document layout.

May 4, 2009 – Non-material changes made:

- Deleted incorrect version number field

June 8, 2010 – Corrected URLs.
