MARIPOSA COUNTY **AGENDA** **DATE:** Feb. 19, 2008
BOARD OF SUPERVISORS **ACTION FORM** AGENDA ITEM NO. CA-1

DEPARTMENT: Technical Services **BY**: Rick Peresan
PHONE: 966 8029

Policy Bk

RECOMMENDED ACTION AND JUSTIFICATION:

Approve the Mariposa County Data Backup / Recovery and Electronically Stored Information Policy.

BACKGROUND AND HISTORY OF BOARD ACTIONS:

The Board has approved previous IT policies as they relate to potential legal requirements.

ALTERNATIVES AND CONSEQUENCES OF NEGATIVE ACTION:

The County could be exposed to potential legal challenges with regard to electronically stored information.

Financial Impact? ( ) Yes (X) No Current FY Cost: $ Annual Recurring Cost: $
Budgeted In Current FY? (x) Yes ( ) No ( ) Partially Funded
Amount in Budget: $ _____
Additional Funding Needed: $0
Source:

Internal Transfer _____
Unanticipated Revenue _____ 4/5's vote
Transfer Between Funds _____ 4/5's vote
Contingency _____ 4/5's vote
( ) General ( ) Other

List Attachments, number pages consecutively
Cover Letter
Mariposa County Data Backup / Recovery and Electronically Stored Information Policy

CLERK'S USE ONLY:
Res. No.: 08-63 Ord. No. _____
Vote – Ayes: 5 Noes: _____
Absent: _____
(x) Approved
( ) Minute Order Attached ( ) No Action Necessary

The foregoing instrument is a correct copy of the original on file in this office.
Date: _____
Attest: MARGIE WILLIAMS, Clerk of the Board
County of Mariposa, State of California
By: _____
Deputy

COUNTY ADMINISTRATIVE OFFICER:
✓ Requested Action Recommended
_____ No Opinion
Comments:

CAO: _____

MARIPOSA COUNTY TECHNICAL SERVICES

To: Mariposa County Board of Supervisors

From: Rick Peresan, Technical Services Director

Date: February 6, 2008

RE: Data Backup / Recovery and Electronically Stored Information Policy

County Counsel distributed a memorandum on September 11, 2007 regarding electronically stored information and amendments to the Federal rules of civil procedure (FRCP). Those amendments necessitate the County to be attentive, to how it creates, locates, retains, discloses and destroys electronically stored information (ESI). To that end, I conducted a formal review of electronically stored information here in Mariposa County.

Many of the items in that analysis, if made public, could compromise County information security and is not included in support of this agenda item.

However, in summary:

- Mariposa County has business offices in 26 locations. Each of these offices has at least one computer with most having several devices. Of the 26 locations, 24 have connectivity to the County network with varying degrees of access
- In total, Mariposa County has in excess of 300 personal computers.
- 9 locations have direct (Local Area Network) access to central file servers
- 9 locations house a file server for department file access
- 2 locations have a file server and PCs administered by the State of California and is not within the Control of Mariposa County.
- 1 location has a file server and PCs under the authority of a third party.
- Mariposa County Technical Services administers 14 central servers and about 225 PCs
- The Human Services Network Administrator oversees 6 servers and about 75 PCs
- An unknown amount of portable storage devices are in use in the County.

I believe the attached policy demonstrates Mariposa County's intent to adhere to the FRCP rules and supports what is reasonably accessible in the event of litigation.

Mariposa County
Data Back Up / Recovery and Electronically Stored Information Policy

January 30, 2008

1. Policy Overview

Mariposa County requires that all information stored electronically in computerized form is backed up periodically to ensure its safety in the event of a severe hardware interruption, software interruption, virus attack, and any other man made or natural disasters. Our policy is to store all County data on a network drive wherever possible. Operating system and application software that is necessary to access, recreate, or generate the information must periodically be backed up. Backup frequency depends on the significance of the information and its frequency of change. Current copies of backup media will be stored off site.

2. Policy Description

The concept of performing backups of data files and programs is as fundamental as any concept in information services. Information Owners drive the process and 'own' the responsibility that Technical Services covers their business requirements.

Backup procedures should include the following:

- Maintaining a copy of backups off site at all times
- Backing up systems on a daily basis
- Backing up all necessary data files and programs to recreate the operating environment
- Storing the current copy of backups off organization premises
- Storing backup copies at an off-site location sufficiently distant from the data center to ensure their protection if the original system is destroyed.
- Considering the ease of access and retrieval from the off-site storage location, including blockage by debris, transportation, and hours of operation
- Backing up the printed documentation and preprinted forms necessary for recovery
- Having at least three generations of backup tapes so an earlier generation of backup can be used if the current backup media are damaged or become unreadable
- Ensuring that backup is not continually performed on the same set of tapes
- Testing the backup to determine if data files and programs can be recovered
- Personnel must be identified and trained to perform data and/or system recovery
- Backing up on media that are compatible with the alternate computer system that will be used following a disaster, considering storage density, media type, and type of tape or disk drive

NOTE: Voice mail messages are not routinely backed up for the purpose of recovery.
Email data is defined in the Mariposa County Email Retention Policy and is for the purposes of disaster recovery only.

3. Policy Responsibilities

This policy provides guidelines for procedures and responsibilities for management, system administrators, all users, and information technology (IT) services.

Technical Services Director

- Identify computerized systems that store information
- Implement standard frequency of backup for each type of computer system or platform in use based on the significance of the information and its frequency of change
- Implement procedures for transferring the most current copy of backup media to a physically and environmentally secure off-site storage location.
- Monitor backup and recovery procedures and practices to ensure compliance with this policy

System Administrators

- Routinely copy operating software, application software, and production information to backup media based on frequencies set by management. This applies to major systems (e.g. mid-range computers, local area network (LAN) or wide area network (WAN) servers, client/server database servers, special-purpose computers) in use by the department.
- Maintain at least three generations of backup media in a "grandfather, father, son" format
- Transport or provide for the transportation and storage of current backup media at an off-site storage location
- Ensure that at least one current copy of backup media is stored off site at all times
- Determine that the off-site storage location has sufficient physical and environmental controls to ensure the safety of backup media
- Develop and implement procedures for maintaining an inventory and tracking the location of backup
- Document and implement procedures for the orderly recovery and restoration of information and its operating environment from backup media

All Users

- Unless access to a network drive is unavailable, critical information is not to be stored on a workstation drive.
- Perform backup procedures on individual workstations routinely, based on frequencies set by department management
- Ensure that current copies of backup media are transported and stored at an off-site storage location on a routine basis

Technical Services

- Copy operating software, application software, and production information to backup media routinely, based on frequencies set by management. This applies to major systems (e.g., mid-range computers, LAN or WAN servers, client/server database servers, special-purpose computers) in use at the organization
- To ensure complete restoration of servers for disaster recovery, images of production servers should periodically be created and store offsite
- Backup detailed hardware specifications of servers for disaster recovery
- Maintain at least three generations of backup media in a "grandfather, father, son" format
- Transport and store (or provide for the transportation and storage of) current backup media at an off-site storage location
- Ensure that at least one copy of backup media is stored off site at all times
- Determine that the off-site storage location has sufficient physical and environmental controls to ensure the safety of backup media
- Develop and implement procedures for maintaining an inventory and tracking the location of backup media
- Document and implement procedures for the orderly recovery and restoration of information and its operating environment from backup media

4. Electronically Stored Information (ESI) / Litigation Policy

- Current Law. Under statutes, court rules and common law, the County of Mariposa is under an obligation to preserve pertinent physical evidence during and in anticipation of litigation. This obligation extends to documents, records and electronically stored information, including related embedded data and metadata. It is the policy of the County of Mariposa to appropriately locate, retain, preserve, retrieve and produce such physical evidence including ESI during and in anticipation of litigation.

- Purpose. For the purposes of this policy, records are defined as papers, maps, exhibits, magnetic or paper tapes, microfilm photographic films and prints, electronically stored information and other documents produced, received, owned or used by an agency, regardless of physical characteristics. For purpose of this policy, ESI means writing, drawings, graphs, charts, photographs, sound recordings, images and other data or data complications stored in any medium from which information can be obtained, translated (if necessary) into a reasonably usable form in which are within the possession, custody, or control of the County and includes embedded data and metadata.

- Record Retentiongulation. Most departmental records are regulated by state codes or other regulations. Further information may be found at the California Secretary of State's website, where a handbook regarding *Local Government Records Management Guidelines* is available for downloading.

- Litigation Retention. Notwithstanding any provisions of this policy, records, including ESI (together with embedded data and metadata) shall be retained and safeguarded and shall not be destroyed, upon receipt of direction from Risk Management, County Counsel, or the County's litigation counsel to retain particular records relating to anticipated or existing litigation.

- Notification. Upon receipt of any law suit or claim a copy of the lawsuit or claim will be forwarded by Risk Management to the department head(s) of the affected department(s).

- Procedures. Upon notice of suit from Risk Management County departments shall retain and safeguard physical evidence, including documents and records relating to anticipated or existing litigation. This includes the retention and safeguarding of ESI. ESI shall be retained in a reasonably usable form, including embedded data and metadata. Production of the physical evidence, documents, records or ESI shall be coordinated with Risk Management, County Counsel or the County's litigation counsel, as appropriate.

- Destruction of documents. Until advised by Risk Management or County Counsel of the conclusion of a lawsuit or claim, ESI and documents shall not be destroyed.