CALIFORNIA RURAL WATER ASSOCIATION
MEMBERGUARD
Serviced by Glatfelter Public Practice

RISK COMMUNIQUÉ

A technical reference bulletin by the Risk Control Services Department of the Glatfelter Insurance Group

Electronic Data Processing System Protection

The preservation of records is important as these records represent a lot of effort by the staff to establish budgets, document decisions, establish business plans, and communicate with the community. Contingency planning is important to enable the organization to "come back up to speed" following an unanticipated interruption or damage to the building, facilities, and the data systems. Each organization should identify those electronic records that are critical to continued operations, and those records that would be expensive or difficult to recreate. Once these records are identified the following risk management techniques should be evaluated for applicability to your organization.

- Important documents should be electronically backed up and moved off site on a regular basis. A few options for backing up include:
  - Having a duplicate server in another building that automatically replicates the files on an ongoing or periodic basis.
  - Making electronic copies onto floppy disks, CD's or tapes and carrying them offsite for storage in another building. Preferably stored in a fire resistant safe, or protected room.
  - The frequency of back up should ideally be daily, but weekly is a common practice. The frequency can be increased to daily during the end of the tax and billing season.
- Electronic data processing centers should be protected by gaseous extinguishing systems (not wet sprinklers), and they should be located in areas that are subdivided and protected from the other areas of the building.
- Power surge protection for the building and for the specific computer equipment should be provided to reduce the chance of lightning or power surges damaging the sensitive electronic equipment.
- Contracts can be initiated with offsite EDP data warehouse companies who specialize in securing and protecting the backup data. Likewise, outside companies will offer contracts to provide temporary replacement systems while a damaged system is being rebuilt or replaced.
- The primary data systems within the organization should be connected to an uninterrupted power supply such as the emergency generator or a battery backup system.
- The server room should have adequate heating and cooling systems to maintain the temperatures within the manufacturer's specified range. Temperature monitoring alarms should be tied into a central station alarm service. Significant losses have occurred from overheating of computer servers, and back-up power for air-conditioning systems is recommended.

Other considerations include:

- Provide a secure site for storage of laptops, and related equipment and programs as these are attractive items for theft.
- Assure that the access to the systems is thoroughly evaluated for privacy and "need to know". Staff should have secure passwords, and authorization to information should be restricted so that private information is accessible only to those who need access to perform their professional responsibilities.

This is a sample guideline furnished to you by MemberGuard. Your organization should review it and make the necessary modifications to meet the needs of your organization. The intent of this guideline is to assist you in reducing risk exposure to the public, personnel and property. For additional information on this topic, you may contact your Risk Control Representative. www.MyMemberGuard.com