

HARDWARE AND DATA SECURITY

Security for the electronic records created, used, and stored on computer systems is an important issue and a responsibility of the Records Management Coordinators in addition to the Information Technology Managers. The protection of records in whatever format is to be identified on the RRS. This is even more relevant if the data is personal or confidential. Mainframe computer systems have traditionally been protected, but other computers have not because they are frequently considered single-user devices.

As a result, security weaknesses may threaten the confidentiality, integrity, or availability of electronic information. There are two major means of protecting electronic records:

- Physical security of the computer hardware.
- Securing data through controlling access.

Data Concerns

A good security system for protecting electronic data will employ a number of different products, services, and resources, which are customized to an agency's particular needs. Not every system or device is appropriate for all agencies. Those responsible for implementing security systems must weigh the potential costs of suffering a loss. Then, consider the value of each method and develop a complete security system that is tailored for the situation. In order to be successful, computer security has to be an on-going management concern.

NOTE: For information on "Common Methods of Computer and Data Security That Can Be Employed to Customize a Security System" please see Appendix 3 of this Handbook.

Environmental Considerations

The effects of environmental conditions, e.g., humidity, temperature, and cleanliness--on electronic recordskeeping and information processing system components are a security concern because of the potential loss or alteration of records maintained electronically.

A large-scale recordskeeping and information processing operation maintaining great numbers of sensitive records on a large computer will require extensive environmental controls.

A smaller scale, noncritical system operating on a computer will probably involve fewer environmental considerations. However, small systems with sensitive electronic equipment require at least a minimum level of environmental control to operate reliably.

NOTE: Appendix 4 of this Handbook includes the "Environmental Checklist for Establishing an Electronic Recordskeeping System," which should be consulted for routine environmental factors to be considered.

DISASTER PREPAREDNESS AND RECOVERY

Aside from the routine management of electronic records, attention should be given to preparing for disasters. The Emergency Plan of the State of California directs all levels of government to identify, organize and protect their essential and/or vital records. As such, agencies need to develop plans for coping with emergency situations, from minor disruptions to major disasters, to ensure the continued operation of electronic recordskeeping and information processing systems. The records management plan should include disaster preparedness and recovery needs and incorporate this specific plan as a component of the overall records management plan. Contact CalRIM to obtain a copy of the Vital Records Protection and Disaster Recovery handbook for further guidelines.

Disaster recovery planning anticipates how various disasters could threaten records integrity and availability. For example:

- How likely is a disaster to happen?
- What can be done if a disaster does happen?
- What can be done to lessen the impact?
- What can be done to protect records and prepare for recovery in the event of a disaster?
- Consider using project management methodologies to assess and plan to manage risks. Additional information is available on-line from the Project Management Institute at www.pmi.org.

Assessment of Emergency Situations

Emergencies can range from a temporary disruption of power to complete destruction of an office and its occupants. No contingency plan will provide options for all types of emergencies. Planners must determine which of the types of emergencies are most likely to disrupt their operations, and gear emergency response procedures and recovery planning to expected situations.

Not every emergency can be classified as a disaster, but personnel prepared for a disaster can successfully cope with lesser emergencies.

Commonly, four levels of disruption define the severity of an emergency:

- **Limited.** A temporary interruption with no damage or loss can be classified at this level. Examples would be a power failure or fluctuation, a communications failure, evacuation of a site because of a threat, or the unavailability of key personnel.
- **Serious.** Repairable damage to equipment or the office area or replaceable loss of key people, data, records, or software could be considered a serious disruption. Examples would be an equipment breakdown, a failure of the air-conditioning system, or minor damage because of sabotage, vandalism, or human error.
- **Major.** Destruction of equipment or office area or of data can be classified as a major disruption. Examples would be a complete loss of equipment because of water damage, explosion, or structural mishap, or an accidental or deliberate loss of data.
- **Catastrophic.** This category includes the total loss of office area or equipment, data, or people. An example would be the complete destruction of the office and the loss of personnel because of fire or a natural disaster.

Disaster Recovery

Contingency plans must be broad enough in scope to cope successfully with the immediate emergency, provide interim service, and bring the electronic recordskeeping and information processing functions back to normal. Because an organization must respond quickly to a disaster, recovery procedures must be spelled out clearly.

The individuals most likely to execute an emergency plan are the ones who develop it. Developers must consider the possibility that assigned office workers may be incapacitated and unable to function following a disaster. Therefore, the plan should be written so that others less familiar with the office will have the information they need to continue operations.

Disasters resulting in severe damage to an office and its equipment may be required to assume operations at an alternate location until repairs are completed and services are restored.

Planned Backup of Electronic Records

With or without an Electronic Recordskeeping System, agencies will need to ensure that the records have been protected from disaster. Part of the disaster recovery plan will be the planned backup of agency electronic records. Several methods for providing backup are of use for different levels of data protection.

The most important factor in a backup program is to do it regularly.

"How often should I do a backup?" is a common question. The answer is a subjective one, but it can be safely said that the interval between backups is the amount of work you are willing to do over. A rule of thumb in general usage is every eight hours. Backup systems and methodologies vary, but most perform the backup programmatically (automatically) at prescribed times. So, if the computer is used all day long, then backup at least daily. If eight hours of data creation are done in a week, then back up weekly, and so on.

When users share a computer, they should be encouraged to back up their files more often, preferably after every update.

Almost as important as regular backups is labeling backup media accurately so that the following information is available for system restoration:

- Name of the organizational unit responsible for the records.
- Descriptive title of the contents.
- Dates of creation.
- Confidentiality and release information.
- Identification of the software and hardware used.

To be accessible in case of disaster, backup media must be stored in a carefully planned manner. Not only must records be backed up and stored, but agencies must also have copies of current versions of application software for essential systems and up-to-date operations manuals, system documentation, program documentation, and operating system tapes or disks.

A typical backup would consist of establishing three versions of data: the previous generation of data, the active data and a copy of the active data. Backup media should be stored off-site.

While backups provide for records protection, they do not necessarily provide for quick recovery and knowledge concerning records disposition. Electronic Recordskeeping Systems best provide for recovery and disposition.

Steps for Salvaging Damaged Records

If the circumstances require the salvaging of water-damaged electronic media, they should not be used until thoroughly cleaned and dried. This will avoid damage to equipment, especially disk drives.

Magnetic tapes, which have become wet, have a good chance for information recovery. Hand dry all external surfaces with a soft, lint-proof cloth and air-dry the tape using a tape cleaner or winder to run the tapes from reel-to-reel. A company specializing in magnetic tape restoration should be consulted.

Drain and blot floppy diskettes with soft, lint-proof cloth. Peel the jacket away from diskette and rinse the diskette with distilled water. Drain the diskette and place flat; blot and air-dry approximately eight hours. When the disk is dry, insert it into new jacket and copy the data to new diskette and/or other storage device (DVD, CD ROM, Optical disk, hard drive, etc). If the information is copied properly, discard the damaged diskette. Clean copy equipment drive heads to prevent permanent damage.

Disaster Recovery Plan

Refer to the sample format of a "Records Management Disaster Recovery Plan" in Appendix 8 of this Handbook. Please note, it is important to adapt the detailed content of each developed plan section to suit the needs of the individual agency.

State Records Center Disaster Services

The State Records Center is available for disaster recovery storage and vital records services to state agencies. Electronic backups can be delivered by an agency, as often as daily and stored at the State Records Center. Please note there is no specifically designed vault available for magnetic media. Contact the State Records Center for additional information.

CARE OF STORAGE MEDIA AND TRANSMISSION SYSTEMS

How electronic records should be stored depends on their use. The maintenance of electronic records is similar to paper records. Current records are actively used in the office for the day-to-day operations of the agency. There may also be a period of less activity when storage is needed.

There are many types of storage media for electronic records: magnetic media, optical disks, CD-ROM, and DVD. Magnetic media, commonly used for storage of state records, include hard disks, diskettes (floppy disks), and magnetic tape (cartridges). The Media Standards, Appendix 11 of this Handbook, lists recognized standards for various media.

Migration

Migration is a strategy for avoiding the obsolescence of media that is used as a repository for records and/or specific file types (i.e., MS Word “doc”). The media type can become obsolete and current software will not work with it. A migration program needs to put into practice that will insure that files are moved to a current format, preserving the content. This must be done before the media type becomes obsolete. Therefore, electronic records should be periodically migrated to stable media and stable file types within an organization’s overall records management plan.

Media and file types must provide a reliable and stable repository for the authentic record to be preserved and accessible by using current equipment, methods and/or technology, consistent with the DGS “Specifications for Electronic Record Management Software.”

Because media and file types vary widely, a migration strategy should establish a schedule for each media and file type individually, e.g., WordPerfect files might require review and migration to current word-processing software within four years from the date created.

Records management best practices provide that records migration is ultimately justified, even if some of the attributes of a record do not lend themselves well to the migration process, in the preservation of content and utility. The records management methodology implemented and employed in the life cycle of records ensures the security, protection, preservation, and future accessibility of information.

Migration of records is essential to guaranteeing long-term access and the preservation of valuable records. To insure that records can be migrated, records management best practices encourage the use of open systems, standard-compliant technology, and wise

budgeting that accounts for training and technology upgrades, selection of dependable software, and sound management of the system.

In California State government, the Secretary of State, California State Archives must in part, rely upon the best practices of the records manager. If the records manager fails to properly maintain records, the archivist's role in the preservation of the record is compromised. If records are earmarked by the Secretary of State (via approved records retention schedules) have been migrated to a different media and/or file type, and the old media containing the records is no longer needed, the media and its contents should be made available to the California State Archives. Absolutely no such media should be destroyed without the approval of the State Archivist.

Hard Disk Maintenance

Hard disks offer on-line, immediate access to electronic records. A hard disk's advantage over a diskette is its speed and storage capacity. While similar to a floppy disk in magnetic surface, hard disks are solid. As a result, hard disks can spin much faster than diskettes. Hard disks reach speeds of 7200 revolutions per minute (rpm) and higher compared to about 300 rpm for a floppy disk.

The hard disk is more sensitive than a diskette. The smallest pieces of dust or smoke can damage the disk. Data may also be lost if a computer is subject to rough handling. This is because information is recorded to and from the hard disk by the disk drive's read/write head, which sits very close to the disk's surface but should not make contact with it. If contact between the disk and the read/write head does occur, it will probably cause severe damage by scratching the recording surface of the disk. This is one of the reasons for what is called a head crash (loss of data on the hard disk).

Always move the computer with care. Most hard disks provide a designated landing zone on which the disk head can be parked when moving the system to reduce the risk of a head crash. Some systems automatically park the head each time the system is turned off. The documentation for the computer should include specific instructions for protecting the hard disk during a move.

Another potential problem for hard disk usage is fragmentation. Through the daily creation and deletion of files, the data on hard disks becomes fragmented, which decreases disk performance (speed) and could eventually result in a head crash. Operating system instructions include procedures for reducing fragmentation. There are commercial utilities, which are simple and easy to use to "tune-up" the hard disk.

NOTE: The information recorded on a hard disk is subject to error, or even totally lost, if a device that emits a magnetic force is placed near the computer's hard disk. This also applies to electronic records stored on all types of magnetic media.

Diskettes

Diskettes are the most common storage devices for personal computers because they are inexpensive and can be reused, transported, and filed. Diskettes can have the same problem with fragmentation as was previously discussed concerning hard disks. A periodic erasure and reformatting of the diskette prior to copying files off of the hard disk can help prevent a floppy disk crash. Diskettes are delicate and require special care. For further information, refer to "Care of Diskettes" in Appendix 5 of this Handbook.

Magnetic Tape and Cartridges

Magnetic tape and tape cartridges are generally associated with large mainframe or minicomputer operations. The records residing in computers are increasingly being transferred to tape on larger computers to provide a backup copy. Computers often use cartridges, or "streaming tape," for a backup copy instead of floppy disks. Like the surface of diskettes and hard disks, magnetic tape is coated with an emulsion of magnetic oxide particles. Other chemicals are also used in the manufacturing process to give the tape good operation characteristics, such as flexibility, conductivity, and softness.

Computer magnetic tape is a fragile medium, highly susceptible to the generation of error by improper care and handling. The complete care and maintenance of magnetic tape can be a complicated and involved process. Even under ideal conditions of controlled storage, magnetic tape is not expected to retain data in a readable state any longer than 10 years. For further information, see the "Common Causes of Tape Damage and Data Loss" in Appendix 6 of this Handbook.

Optical Disks

Optical disk technology offers a stable media environment as compared to magnetic hard drives. Read/write optical disk systems provide a supplement, complement, or alternative to magnetic storage media in a broad spectrum of data and document storage applications. These systems permit the direct recording of information generated by keyboards, document scanners, and other input devices. They can also record information transferred from magnetic media and other optical media, or downloaded from a mainframe.

Read/write optical disk systems include both equipment and media. Optical disk drives are readily available for purchase as computer peripheral devices.

Considerable additional engineering and programming expertise may be required for the hardware customization and software development necessary to combine scanners, computers, optical media, video displays, printers, and other components into an effective document storage and retrieval system. Read/write optical media can be divided into write-once and erasable varieties. Write-once optical disks record irremovable information. Erasable optical disks, like their magnetic counterparts, permit reuse of previously recorded media segments.

Optical disks resemble a phonograph record/platter and are available in 12-inch, 8-inch, and 5.25-inch sizes; the sizes change depending upon the manufacturer and the technology. There has been very little standardization in the design of this media. CD-ROM and DVD are also optical disks (media) but due to their popularity in the entertainment industry this media is very standardized and can be used with a wide variety of equipment.

Optical disks differ in materials, construction, thickness, etc. Regardless of recording technology or media source, write-once optical disks are enclosed in plastic cartridges to facilitate handling and protect them from environmental contaminants. A laser beam "writes" data onto the disk. The information is represented on the disk by a change in the surface reflectivity and is read by using a low-powered laser to sense the changes. Optical disks have recording surfaces on either one side or both sides, with dual sides being the most common.

The World Wide Web & Internet

The Internet is a communications method or protocol that links servers and the individual computers attached to them. The Web page is a document residing on a server that contains text, graphics, animations and videos. All servers use hypertext markup computer language to permit them to display the Web page information on the screen of the individual user. Various pages of hypertext are linked together on a single server.

As the Web pages and the data that is captured from them become the substitute for paper transactions, retention periods and methodology will need to be applied as with other electronic records. The use of agency websites to communicate information to the public may be important records, which need to be managed and addressed in records retention schedules.

Note: For more information on the WWW, please see Appendix 12.