

### **APPENDIX 3 - COMMON METHODS OF COMPUTER AND DATA SECURITY THAT CAN BE EMPLOYED TO CUSTOMIZE A SECURITY SYSTEM:**

- **Risk Analysis.** Software packages are available to help quantify potential exposure to security breaches. This is a good starting point in determining your need for and development of a plan of action.
- **Access Levels.** Users can be assigned a variety of access privileges, such as read only, remote access, specific file or directory access, and ability to upload or download data from a mainframe or network database.
- **Passwords.** Passwords can be used to control access to terminals, files, records, or even fields within a record. In a password system, users must enter the appropriate password to gain access to the data for which they have been cleared. Multiple levels of passwords can provide entry to different layers of information in an agency database. The best approach is to use passwords to create a hierarchy of entry and progressively more complex entry codes, as the information becomes more sensitive.
- **Callbacks.** Callback devices prevent unauthorized access to the communications channels of a computer. Some devices require a caller to provide an identification number and hang up. After verifying the user's access rights, the device calls the user back. When combined with a password, the system requires that the correct user identification also be provided from a specific location (modem number).
- **Audit Trails.** Security software programs can audit computer use by providing a comprehensive record of all network or system activity, including who is accessing what data, when, and how often.
- **Encryption.** Data encryption is a process that "scrambles" data when it is stored or transmitted. Data so treated become unintelligible without a data "key." When the encrypted data are sent to another terminal, the required software key on the receiving end decodes the information. The use of encryption can be a complex process and should be used only for data that is highly confidential and require utmost security.
- **Data Backups.** Backing up disks will be discussed later in the Disaster Preparedness and Recovery section of this handbook as a common-sense measure to safeguard data in the event of loss through disaster. It is also important for basic computer security. Data backup is an important safeguard should an unauthorized user access and change an electronic file or document.
- **Security Levels.** Distinguishing the levels of security for records (confidential, personal, or open) is useful for determining each records series' appropriate level of protection. Access by the public to records in the custody of state agencies is covered

by the Public Records Act (Government Code Section 6250 et seq.). The Public Records Act basically states that all Public Records are open to inspection at all times during the office hours of the state or local agency and every citizen has a right to inspect any public record, except as noted. It further states that every agency may adopt regulations stating the procedures to be followed when making its records available in accordance with the Act.

*NOTE: Electronic records that are confidential according to the Information Practices Act (Civil Code Section 1798, et seq.) or because of federal regulations or law, such as the Privacy Act of 1974, should not be maintained on computers that can be accessed by anyone in the office.*

## **APPENDIX 4 - CHECKLIST FOR PRE-PURCHASE CONSIDERATIONS AND REVIEWS FOR ELECTRONIC RECORDSKEEPING SYSTEMS**

### **Requirements Analysis:**

- What is it exactly that we want the new or modified system to do?
- Do we really need it?
- Will the proposal further accomplish the agency's mission?
- What advantages will it provide?
- What problems will be solved?
- Is there money budgeted for it?

### **Feasibility Considerations:**

- Is the system we are planning or proposing within the realm of possibility?
- Have such things as space, electrical requirements, and other environmental factors been taken into consideration?
- Are the personnel available?
- What additional training will be necessary?

### **Cost Benefit Analysis:**

- Will the cost of what we are proposing be more or less than the benefits derived?

### **Consideration of Equipment Alternatives:**

- Does other equipment exist that could do the same or a better job at a similar or reduced cost?

### **Compatibility Considerations:**

- Are the computers used for electronic recordskeeping able to communicate among themselves?
- Are they able to exchange and manipulate information by using the same operating system?
- Are there plans for networking some or all of the equipment?
- Is there a need to communicate between or among other pieces of similar equipment?

**Disposition:**

- Have provisions been made for the authorized disposition of records determined by an approved records retention schedule?

**Security:**

- Has adequate security been provided for the electronic records and equipment?
- Does the potential for misuse or unauthorized disclosure, modification, or destruction require this material to be afforded greater protection than other office equipment and records?

**Standards:**

- Does the electronic recordskeeping system being considered meet or exceed the DGS “Specifications for Electronic Records Management?”

**(Source:** *Electronic Recordskeeping*, U.S. General Services Administration)

## **APPENDIX 5 - ENVIRONMENTAL CHECKLIST FOR ESTABLISHING AN ELECTRONIC RECORDSKEEPING SYSTEM**

- Provide reliable electrical power for the equipment processing electronic records. A dedicated power circuit may be needed for the dependable operation of the equipment. Install electrical surge protectors to counter or cope with utility power fluctuations. Establish backup power sources such as auxiliary electrical generators or battery systems, if power outages are a problem.
- Install/Decide if cooling, heating, dust, or humidity control equipment is needed at the record processing or storage sites.
- Determine if static electricity discharges are likely to cause data losses at electronic record processing or storage sites. The danger of static electricity can be minimized with antistatic sprays, carpets, or pads.
- Prohibit eating or drinking in the immediate vicinity of the records media and the processing equipment. These restrictions prevent contaminants from harming the records or equipment.
- Install fire protection systems, as needed, in electronic records processing and storage facilities.
- Determine if physical security measures, such as door locks or intrusion alarms, are needed at electronic recordskeeping sites.
- Plan for the secure offsite storage of backup copies of valuable electronic records.
- Obtain special furniture, such as printer stands or magnetic tape rack, to help provide for the effective operation of the recordskeeping system.

**(Source:** *Electronic Recordskeeping*, U.S. General Services Administration)

## **APPENDIX 6 - CARE OF DISKETTES**

- Maintain storage temperatures between 50 and 120 Fahrenheit.
- Avoid disk contact with equipment generating magnetic fields, such as telephones.
- Protect disks from direct sunlight.
- Avoid using clips of any kind to attach things to floppy disk.
- Protect disks from liquids or dampness.
- Do not bend or handle roughly.
- Do not touch exposed portions of a disk.
- Do not lay metal objects on a disk.
- Use care when inserting a disk into or removing a disk from a computer's disk drive.
- Store disks vertically in a rigid container that is not vulnerable to light and dust.

**(Source:** *Electronic Recordskeeping*, U.S. General Services Administration)

## **APPENDIX 7 - COMMON CAUSES OF TAPE DAMAGE AND DATA LOSS**

- Physical mishandling by operational personnel.
- Failure to properly label recorded tapes.
- Poor on-site maintenance.
- Failure to control the temperature and the humidity in the storage area or during use.
- Contamination, debris, and cumulative wear products in the tape pack caused by poor tape manufacturing control, operator mishandling, and defective tape transport components.
- Maladjusted or misaligned transports or other tape winding equipment that caused improper tape tensioning and winding.
- Lack of environmental cleanliness and failure to adhere to proper clean operating practices.
- Subjecting recorded tape to close-in, high-intensity magnetic fields.
- Failure to properly select and pretest tape for use in long-term storage.
- Improper preparation of tape for shipment.
- Lack of protective measures against catastrophic events, such as fire and floods.
- Failure to provide a proper tape and system maintenance schedule.
- Failure to perform visual inspection of the tape, tape reel flanges, and hubs before operation and storage.
- Failure to properly clean and evaluate tapes before using.
- Failure to sample three percent of holdings annually to determine condition of data and to periodically recopy older tapes.
- Failure to periodically rewind tapes at constant tension, at normal tape speed.

- Failure to copy data on the tapes to new or re-certified tapes at least once every two years or more frequently when necessary to prevent the physical loss of data or technological obsolescence of the medium.

**(Source:** Electronic Recordskeeping, U.S. General Services Administration)

## **APPENDIX 8 - RECORDS INVENTORY WORKSHEET, STD. FORM 70**

You may view, fill out, and print this form online at

<http://www.osp.dgs.ca.gov/pdf/std070.pdf>.

**APPENDIX 9 – SAMPLE RECORDS MANAGEMENT DISASTER RECOVERY PLAN**

**I. Name of agency:** \_\_\_\_\_

**II. Date of completion or update of this plan:** \_\_\_\_\_

**III. Agency staff to be called in the event of a disaster:**

<b>Position Numbers</b>	<b>Name</b>	<b>Telephone  (Home and Office)</b>
-----------------------------	-------------	---

Disaster recovery team:

Leader \_\_\_\_\_

Members/alternates \_\_\_\_\_

---

---

---

---

---

---

---

---

---

---

Building maintenance \_\_\_\_\_

Building security \_\_\_\_\_

Legal advisor \_\_\_\_\_

**Note below who is to call whom upon the discovery of a disaster ("telephone tree"):**

---

---

**RECORDS MANAGEMENT DISASTER RECOVERY PLAN**

**IV. Emergency services to be called (if needed) in the event of a disaster:**

<b>Service</b>	<b>Name of Contact</b>	<b>Telephone Number</b>
Ambulance	_____	_____
Carpenters	_____	_____
Chemist	_____	_____
Data processing backup	_____	_____
Electrician	_____	_____
Emergency management coordinator	_____	_____
Exterminator	_____	_____
Fire department	_____	_____
Food services	_____	_____
Locksmith	_____	_____
Micrographics Contractor	_____	_____
Plumber	_____	_____
Police department	_____	_____
Security personnel (extra)	_____	_____
Software Contractor	_____	_____
Temporary personnel	_____	_____
Utility companies:	Electric _____	_____
	Gas _____	_____
	Water _____	_____
Other individuals and/or organizations to assist in cleanup	_____	_____

---

**RECORDS MANAGEMENT DISASTER RECOVERY PLAN**

**V. Locations of in-house emergency equipment and supplies (attach map or floor plan with locations marked):**

Batteries \_\_\_\_\_

Badges (employee identification) \_\_\_\_\_

Camera and film \_\_\_\_\_

Cut-off switches and valves \_\_\_\_\_

Electric \_\_\_\_\_

Gas \_\_\_\_\_

Water \_\_\_\_\_

Sprinkler system (if separate) \_\_\_\_\_

Extension cords (heavy-duty) \_\_\_\_\_

Fire extinguishers \_\_\_\_\_

First aid kits \_\_\_\_\_

Flashlights \_\_\_\_\_

Ladders \_\_\_\_\_

Mops, sponges, buckets, and brooms \_\_\_\_\_

Nylon monofilament \_\_\_\_\_

Packaging tape and string \_\_\_\_\_

Paper clips (non-rust) \_\_\_\_\_

Paper towels (not colored) \_\_\_\_\_

Pencils/waterproof ballpoint pens \_\_\_\_\_

Plastic trash bags \_\_\_\_\_

Rubber gloves \_\_\_\_\_

Scissors \_\_\_\_\_

**V. Locations of in-house emergency equipment and supplies (attach map or floor plan with locations marked):**

Transistor radio (battery powered) \_\_\_\_\_

Wiping cloths \_\_\_\_\_

Writing tablets \_\_\_\_\_

**VI. Sources of off-site equipment and supplies (if maintained on-site, note location):**

<b>Item Number</b>	<b>Contact/Company</b>	<b>Telephone</b>
CB radio	_____	_____
Dehumidifiers	_____	_____
Drying space	_____	_____
Dust masks	_____	_____
Fans	_____	_____
Forklift	_____	_____
Freezer or wax paper	_____	_____
Freezer space	_____	_____
Fungicides	_____	_____
Generator (portable)	_____	_____
Hard hats	_____	_____
Pallets	_____	_____
Plastic milk crates	_____	_____
Plastic sheeting (heavy)	_____	_____
Pumps (submersion)	_____	_____
Rubber boots or overshoes	_____	_____
Refrigeration truck	_____	_____

**RECORDS MANAGEMENT DISASTER RECOVERY PLAN**

**VI. Sources of off-site equipment and supplies (if maintained on-site, note location):**

<b>Item Number</b>	<b>Contact/Company</b>	<b>Telephone</b>
Safety glasses	_____	_____
Spot lights	_____	_____
Trash cans (plastic, small and large)	_____	_____
Plastic trash bags	_____	_____
Unprinted newsprint	_____	_____
Vacuum/freeze drying facilities	_____	_____
Waterproof clothing	_____	_____
Wet-dry vacuum	_____	_____
Worktables and chairs	_____	_____
Computer equipment	_____	_____

**VII. Salvage priority list:**

Attach a copy of the records retention schedule identifying all vital (essential) records series. The location and record medium of the preservation duplicate for each vital records series should be noted.

It is also very helpful if other records series are reviewed to determine their priority for salvage should a disaster occur. The following questions can be helpful in determining priorities:

- Can the records be replaced? At what cost?
- Would the cost of replacement be less or more than restoration of the records?
- How important are the records to the agency?
- Are the records duplicated elsewhere?

To simplify this process, priorities may be assigned as follows:

- Salvage at all costs, for example, records that are historically valuable or non-vital records that are important to agency operations and very difficult to recreate.

**RECORDS MANAGEMENT DISASTER RECOVERY PLAN**

- Salvage if time and resources permit, for example, records that are less important to the agency or somewhat easier to recreate.
- Dispose of as part of general cleanup, for example, records that do not need to be salvaged because they are convenience copies and the record copy is at another location.

### **VIII. Agency disaster recovery procedures:**

Attach a list of specific procedures to be followed in the event of a disaster in your agency, including responsibilities of in-house recovery team members.

### **IX. Follow-up assessment:**

A written report, including photographs, should be prepared after recovery and attached to a copy of the disaster plan. The report should note the effectiveness of the plan, and should include an evaluation of the sources of supplies and equipment, and of any off-site facilities used.

**(Adapted from:** Basic Guidelines for Disaster Planning in the State of Oklahoma)