How do I protect records from loss or damage?

Physical, environmental, and technological hazards can place UN records and information at risk. When records are lost or the information in them is compromised, your office will struggle to fulfill its mandated responsibilities. Protecting electronic and paper records from loss or damage is essential to ensuring you can carry on your work effectively and efficiently.

When records are lost or damaged, the office is exposed to several significant risks, such as:

- the inability to meet operational goals and objectives (operational risk)
- the failure to document or financial decisions or expenditures adequately (financial risk)
- the loss of status as a reliable, effective, and accountable agency (reputational or image risk)
- the exposure of personnel and facilities to loss or damage (physical or security risk).

Records can be lost as a result of disasters such as fires, floods, earthquakes, explosions, military conflicts, or terrorist attacks. Records can also be damaged by emergencies such as power outages, security breaches, or insect infestations. Also dangerous are seemingly minor situations, such as

- not labeling folders, cabinets, or storage boxes clearly, meaning records cannot be found
- not securing records when personnel leave their positions, hindering the transition for new personnel
- not destroying superseded records systematically, leading to confusion about authoritative versions
- not protecting computer systems with up-to-date anti-virus software, risking data damage or loss
- not imposing strong password controls, leaving gaps in computer security systems.

Preventing disasters

The first step in protecting records is to try to prevent a disaster in the first place. The two most serious disasters are fire and flood, which can be caused by a range of events, such as earthquakes, explosions, arson, overflowing rivers, rising tides, or failed sprinkler systems. The following actions will reduce fire and flood risks.

Reducing the risk of fire

1. Ensure the office complies with all fire regulations.
2. Install fire alarms, smoke detectors, and heat detectors and ensure they are always working.
3. Train personnel in emergency and evacuation procedures and conduct regular training exercises.
4. Ask the fire department to identify weaknesses in fire protection and suggest improvements.
5. Ban smoking or open flames anywhere records are kept.
6. Store flammable liquids in locked metal cabinets or locations removed from people or records.
7. Check electrical wiring, plugs, and cords regularly and replace any worn components.
8. Ensure all storage containers for records are strong, stable, and non-flammable.
9. Keep all records storage areas clean and tidy.
10. Identify and label vital records clearly so they can be retrieved immediately in an emergency.

Reducing the risk of flooding or water damage

1. Do not store records directly below or above heating, water, or drainage pipes.
2. Do not use top shelves for storage and ensure bottom shelves are 6" (15 cm) off the floor.
3. Use high-quality, strong storage boxes, shelves, and containers for records storage.
4. Identify all locations where water might penetrate, and inspect those locations regularly.
5. Regularly check humidity levels in storage areas; increases can be caused by water penetration.
6. Ensure regularly used water taps are always turned off when not in use, anywhere in the office.
7. Turn off central water pipes if the building will not be occupied for any length of time.
8. Regularly inspect and maintain gutters, drains, and pipes.
9. Install flood alarm systems in record storage areas.
10. If possible, store records in a location with a pitched, not flat, roof, so that water drains off.

Managing records securely

To protect both paper and electronic records and ensure valuable records are safe and accessible, follow these basic record-keeping principles.

- Always keep desks and records storage areas clean and free of records when not in use.
- Distinguish between information and records as soon as possible after creating/receiving them: keep records safe for ongoing use and remove non-record information as soon as possible.
- Assign clear and understandable names to all records or file folders so that electronic and paper records can be easily filed and retrieved.
- Destroy duplicates or convenience copies of records as soon as you no longer need them.
- Secure official records securely in authorized record-keeping systems, such as physical or electronic storage repositories, according to established classification systems or file plans.

Protecting electronic records

Electronic records require additional safeguards to protect them from loss or damage. Most important is to work with the IT specialists at UN OICT and the records specialists at UN ARMS to guarantee that computer systems are configured properly, so that electronic records are created, managed, and stored securely and disposed of appropriately. UN OICT will help you ensure that your office has:

- regular and secure backups of all official records.
- robust, high-quality computer firewalls and up-to-date virus protection software
- strong password protection for all computers and related equipment
- data encryption as appropriate to protect sensitive electronic records
- surge protectors and backup systems to protect computers during power outages.

Remember... Simple actions – such as identifying and labeling records clearly, destroying obsolete records, and storing all records securely – can make a tremendous difference to the safety of your office's records. Protecting records from loss or damage is a fundamental part of good records management.

To understand how to protect records in an emergency, see Record and Information Management Guidance Sheet number 9. To understand how to assess the quality of your office's records systems, see Record and Information Management Guidance Sheet number 10.