



## How do I protect records in an emergency?

It is not always possible to prevent an emergency, but you can reduce the likelihood that emergencies become disasters by establishing and following effective emergency management practices.

In 2012, Superstorm Sandy caused widespread damage to large portions of the eastern seaboard of the United States, seriously affecting the UN's operations. But disasters that pose a threat to the UN's personnel and services, and its records, do not have to be widespread or catastrophic events such as earthquakes, tsunamis, or hurricanes. Other threats include fires, bombs, floods, or insect infestations. And security breaches and thefts can also damage paper or electronic records systems and expose the UN to serious risks.

Whatever the cause of an emergency, any threat can endanger the integrity and stability of your office's records. And your office relies on its records to perform its work, fulfill its obligations, and protect the rights and responsibilities of the UN and its personnel, as well as third parties. Therefore, protecting records is critical in an emergency, second only in priority to protecting people. Desks and chairs and tables can be replaced – people, and the records and information they rely on to carry out their duties – cannot.

### How to be prepared in case of emergency

Prevention is the best insurance against the loss of records and information in an emergency. The following steps will help reduce the chance that your office's records will be lost or damaged.

1. Ensure your office records systems are effective, efficient, accountable, and transparent by establishing formal processes for managing all documents and records, regardless of format or medium.
2. Confirm that the building or room in which records are stored is secure, equipped with fire and flood prevention and detection devices, and fitted with locks and alarms.
3. Protect paper records by always storing them in boxes or cabinets in cool, dry, secure locations, ideally away from windows, water pipes, or gas pipes, and at least 6" (15 cm) off the floor.
4. Protect electronic records by establishing and following appropriate backup and storage procedures.
5. Inspect records storage areas regularly to ensure they are secure, safe, and free from any sign of deterioration, infestation, or damage.
6. Ensure all personnel are trained to handle records securely, including adhering to records classification schemes and file plans, cleaning up records according to retention schedules, and protecting sensitive information.
7. Maintain effective records management procedures, including destroying obsolete or superseded records according to established retention schedules, formally transferring archives to UN ARMS, and establishing clear procedures for protecting vital records, so that all office records are well protected and accessible as needed in the event of an emergency.
8. Make sure all personnel are aware of and trained in emergency response procedures.
9. Develop and implement a formal disaster recovery plan, including measures for prevention, recovery, and post-incident reviews. Test the plan regularly and update it to reflect any major office changes.

### Developing a disaster recovery plan

A disaster recovery plan ensures that, in the event of an emergency, your office can act quickly and effectively to protect materials from harm, recover any damaged materials, and prevent further risks to records.

## Elements of a disaster recovery plan

An effective disaster recovery plan will include information about:

- likely disasters and their impact on the records
- preventative measures to reduce the risk of disaster or to mitigate damage as much as possible
- the locations of vital, high-risk, or sensitive records and detailed procedures for protecting them
- emergency contacts, including key personnel, contractors, fire and police departments, and so on
- the identification and management of vital records
- priority actions to help the office resume business operations as soon as possible
- priorities and procedures for salvage and repair of records and information
- procedures for ensuring continued access to critical records during salvage and repair operations
- the best way to integrate records recovery operations with other emergency response priorities
- procedures for rehabilitating damaged storage spaces or containers
- when and how to review and update the disaster recovery plan, so it is always current.

**A disaster recovery plan is different from a vital records plan.** Actions taken to manage the office's records in an emergency involve all the organization's records, not just its vital records. But in practice, both plans should be closely linked, and they should be developed and reviewed at the same time to ensure they are well coordinated. Your office will need to work with all stakeholders to develop a comprehensive disaster recovery plan, and ensure that all personnel are aware of their roles and duties to help execute the plan effectively.

## Taking action after a disaster

In the event of a disaster, the personnel responsible for dealing with records should follow these key steps:

1. Access a copy of the emergency plan.
2. Confirm with senior management that the office is operating under emergency conditions.
3. Bring the disaster response team together and confirm and prioritize recovery operations.
4. Confirm that all personnel are safe.
5. Allocate immediate responsibilities to personnel according to the plan.
6. Establish a disaster response site.
7. Recall, and if necessary reconstitute, vital records and issue them to appropriate personnel for action.
8. Ensure that the office is structurally sound and safe before authorizing anyone else to return.
9. As appropriate, arrange to salvage any non-vital records or clean up records systems or storage areas.
10. Once the disaster is over and the office is back to normal, review the plan and make changes to improve it for next time.



To understand how to protect records from loss or damage, see **Record-keeping Guidance Sheet #8**. To understand how to assess your office's records systems, see **Record-keeping Guidance Sheet #10**.