How do I ensure records are secure?

All UN records – regardless of whether they are in paper or electronic form – must be protected from damage, loss, destruction, misuse, unauthorized disclosure, modification, and other risks.

Whether or not records are unclassified, confidential, or strictly confidential, all personnel in the United Nations must manage records so that they are safe from loss, destruction, or misuse. To help offices across the UN protect all their valuable information assets, the UN Secretariat has implemented a comprehensive information security programme. The goal is to protect information as securely as possible while ensuring personnel across the UN can access information and records in order to carry out their duties effectively.

The following guidance relates specifically to protecting official records. For further advice on managing documents and records, contact the records professionals at UN ARMS. For help on other information security issues, contact the information security professionals at UN OICT.

Understanding levels of risk

The UN is constantly exposed to a variety of risks, including: **operational risk**: the inability to meet operational goals and objectives; **financial risk**: the failure to document financial decisions or expenditures adequately; **reputational or image risk**: the loss of status as a reliable, effective, and accountable agency; and **physical or security risk**: the exposure of personnel and facilities to loss or damage.

The effective management of official records can help eliminate or reduce the impact of these risks, by ensuring your office can provide the evidence you need to prove your actions, confirm operational or financial decisions, demonstrate accountability and transparency, and protect employees and property from harm.

Understanding sensitivity classifications

One of the ways the UN manages risk is to classify documents and records according to levels of sensitivity. The higher the sensitivity of a record, the stringent protection it requires, in order to reduce risk. The UN's sensitivity classifications are as follows:

> **Strictly confidential:** information or material whose unauthorized disclosure could reasonably be expected to cause EXCEPTIONALLY GRAVE DAMAGE TO or IMPEDE THE CONDUCT OF THE WORK of the United Nations.
>
> **Confidential:** information or material whose unauthorized disclosure could reasonably be expected to cause DAMAGE TO THE WORK of the United Nations.
>
> **Unclassified:** information or material whose unauthorized disclosure could reasonably be expected NOT TO CAUSE DAMAGE TO THE WORK of the United Nations.

All the documents and records under your control should be identified according to one of these three sensitivity classifications. These documents and records must be stored and handled so that the information in them is not inappropriately disclosed, whether the information is in paper or electronic form.

Regardless of other specific actions, you should **always use approved records classification schemes and file plans** to ensure records are stored in the right place, whether the records are physical or electronic.

Protecting records in offices and storage areas

Follow these basic security measures to safeguard physical (i.e., paper) documents and records:

1. Fit doors and windows in all offices and records storage areas with strong locks.
2. Keep filing cabinets and other records storage areas locked at all times when not in use.
3. Label all files, folders, and boxes so that their contents, dates, and extent are clear.
4. Equip offices and storage areas with fire and security alarms and test alarms regularly.
5. Only permit access to records storage areas to a small number of qualified personnel.
6. Supervise all external visitors whenever they are in offices or records storage areas.
7. Conduct regular security and facility inspections for all work spaces or records storage areas.
8. Transfer records with ongoing value to UN ARMS according to records retention schedules.
9. Destroy obsolete and superseded records securely as soon as they are no longer needed.
10. Maintain full documentation about all records destroyed or transferred to UN ARMS.

Protecting electronic records

Follow these steps to safeguard electronic documents and records, including emails:

1. Do not use computer hard drives (C: drives) to store sensitive information. Instead, store sensitive information in formally established electronic record-keeping systems or, in the absence of such systems, in secured network drives.

2. Regularly clean up computers and network locations by destroying superseded or obsolete records that have met their retention periods.

3. Recognize that deleting electronic records is not the same as destroying them. Work with the IT specialists at UN OICT and the records specialists at UN ARMS to guarantee that computer systems are configured to ensure that deleted records are permanently removed from network drives or other storage locations.

4. Contact UN OICT for guidance about ensuring your computer systems are configured with appropriate security systems, anti-virus software, password protection, and automatic time out/lock features to restrict access to password holders only.

5. Contact Un ARMS for guidance about how to create, store, and manage electronic records so that they are safe, accessible, and authentic, now and in the future.

Remember... Secure record-keeping involves protecting records as long as they need to be kept, then disposing of them appropriately. Good record-keeping also involves keeping full and accurate documentation about which records were destroyed and which were sent to UN ARMS for permanent preservation.

To understand how to protect records from damage, see Record and Information Management Guidance Sheet number 8.To understand how to protect records in an emergency, see Record and Information Management Guidance Sheet number 9.