Section 18 – Destroying Records

Contents

Main Things to Remember about Destroying Records

- Destruction is the final process which ensures the integrity and credibility of the whole records management system.
- Each mission needs to set up a formal approval process for records destruction.
- All destruction of records should be fully documented.
- Follow ARMS procedures to ensure records are destroyed in a timely fashion, according to retention schedules and authorised by designated departmental officials to appropriately secure standards.
- There need to be mechanisms to delay or change the destruction action date if business units have a justifiable reason.

Introduction

Very few records created by any part of the UN will have the kind of value which warrants their permanent retention as historical archives. All other records (possibly as many as 95%) need to be destroyed securely in a controlled manner. This is not only good practice from a risk management and efficiency perspective but it is essential to complete the recordkeeping cycle.

Information Box

Reasons for Destroying Records

There are many good reasons for destroying records promptly when they are no longer needed:

- To ensure best practice and confidence in the recordkeeping programme
- To demonstrate accountability and consistency in implementing destruction decisions
- To reduce maintenance costs
- To prevent records with no continuing usefulness from slowing down the system (this is particularly relevant to searching for electronic records)
- To eliminate unnecessary storage costs
- To eliminate any risk of sensitive or personal information falling into the wrong hands

The Principles of Records Destruction

ARMS has developed a set of principles which govern records destruction at the UN. The principles specify that records destruction should be:

1. Authorised by both ARMS (through PORS) and by the business unit's internal approval process
2. Appropriate (irreversible and environmentally friendly)
3. Secure/Confidential
4. Timely

5. Documented (so that there is a record of what has been destroyed by what authority and surety that the record(s) have really been destroyed)

There is more detail on each of these principles below. The ARMS' Guideline on Records Destruction also gives more information.

Knowing Which Records to Destroy and When

PORS (Peacekeeping Operations Retention Schedule) determines which records can be destroyed and when destruction of those records should happen.

Using Retention Schedules to Manage Destruction

In peacekeeping operations PORS governs how long to keep your records and what happens to them at the end of the cycle. Although the cycle may involve several stages of transfer to different storage areas (office space, local archives, ARMS storage facilities), at the end of the cycle records are either designated as archives or they are destroyed. Records retention schedules are therefore the instruments which provide the formal disposition authorisation upon which a UN office can act.

Retention schedules give each record series a set of instructions as to where they should be kept and for how long. In the example below, the records series LOG001.P, ***Policy and procedure*** is transferred to the local archive i.e. the mission records storage facility when closed and should be transferred to the Permanent Archive 1 month after the End of Mission Mandate. Clearly these records should not be destroyed! The second record series, ***Reporting to the UN***, is also transferred to the local archive when closed. However, as the schedule clearly states, "**Destroy Permitted**", so the records can be destroyed either 3 years after they are closed or 1 month after the end of the mission. For more information on records retention requirements for UN field missions, refer to the Peacekeeping Operations Retention Schedule (PORS) User Handbook.

Although PORS specifies when records can be destroyed it is essential that there is control over the destruction process. Your mission records management officer will develop a formal approval destruction approval process.

UNITED NATIONS

Retention Schedule for Records of Peacekeeping and Political Missions

January 2006

Definitions: Local Archive = Keep in Office; Interim Archive = Transfer to ARMS; Permanent Archive = Transfer to ARMS for permanent storage *Page 1*

Schedule No.	Title	Transfer	Destruction	Notes	Source	Active
LOG001.P	Policy and procedure	Local Archive after Date closed Permanent Archive 1 month after End of Mission Mandate	**Must Not Destroy**		**PPM**	Active –Schedule has been active since 30/09/2005
LOG002.P	Reporting to UNHQ	Local Archive after Date closed	**Destroy Permitted** Destroy 3 years after Date Closed Destroy 1 month after End of Mission Mandate (User Defined)	Office of record: UNHQ DPKO/OMS/LSD	**PPM**	Active –Schedule has been active since 25/08/2005

Agreements with ARMS about Retention

If mission staff cannot identify retention instructions in PORS, your mission records management officer should contact ARMS staff to discuss adding the series to the PORS.

When to Destroy Records

Records should not be destroyed while there is still a need for them but they should not be kept any longer than is necessary for legal, regulatory or business reasons. Records are usually destroyed when they have reached the end of a specified retention period, as discussed above. However, before destroying records, a procedure should be implemented requiring the creating office to give signed approval for destruction.

Destruction of Records from the Business Unit

Information Box

"The PORS [the Peacekeeping Operations Records Retention Schedule]… permits the destruction of records in the mission area, thus mitigating the costs of shipping and rented storage space in New York, both of which obligated from mission budgets"

Peacekeeping Operations Retention Schedule (PORS) User Handbook

If your retention schedule states "**Destroy Permitted**", you may destroy records without further approval from ARMS or DPKO by following your mission's formal approval process for records destruction. However, remember that the disposal schedules set a minimum period for retention, and it is possible that the records may need to be kept for longer. There are 3 main reasons for this:

1. your business unit still has a business or administrative needs for the records
2. the records are required for current or pending subpoena action or the records may be required as evidence in an internal or external investigation
3. the records are the subject of an access request

You can make sure that there are no outstanding reasons to retain the records due for destruction by ensuring you have appropriate internal authorisation or approval processes in place. For example you can provide appropriate staff with lists of records due for destruction.

Once you are certain there are no remaining requirements to retain the records, an appropriate officer should give the final approval for the destruction of records. You should ensure that the business unit has a nominated officer responsible for this process.

Information Box

Responsibility for Authorising Destruction

The person who authorises destruction should be someone who principally either created or used the records in question. They are known as the responsible official or officer.

The single exception is DPKO mission financial records: Field Finance Procedure Guidelines (2001) (Section 2.11.1) "... no records should be destroyed without the prior approval of [DM/OPPBA/Peacekeeping] Accounts Division."

In the case of liquidated missions, the responsible official is someone at UNHQ DPKO familiar with the record series.

If in any doubt about authorising destruction, you should consult your records management officer who is the office of record for all of these records and is familiar with ARMS record destruction procedures.

You must also document all records destruction to ensure that you are complying with best practice and that you and the UN are protected in case of any investigation or query. The documentation not only assists if there is ever any question as to why records no longer exist but also it saves time spent searching fruitlessly for destroyed records. Proof of destruction may be required in investigation proceedings or in response to access requests. If you have an agreed retention schedule and you have obtained the necessary authorization from your business unit, the documentation will provide evidence for best practice recordkeeping and demonstrate consistent and accountable practices.

You will need the following documentation:

- A list or summary details of the type and quantity of records destroyed
- The PORS schedule authorizing destruction (schedule number)

- Proof of destruction (e.g. certificate), method of destruction and date destroyed

You can use the destruction form at the end of the section, together with detailed lists and any certificates, if you have them, to document your destruction.

More information is given below on technical destruction requirements and procuring contractors to carry out destruction as necessary.

Destruction of Records via ARMS

Missions with long-term mandates that have transferred records to ARMS may occasionally be requested to approve disposal via ARMS. In these cases, during the final year of the records' retention period, ARMS sends you a copy of the RMS 33 accession control form and requests that if you agree to the destruction that you sign at the bottom of the form. As with records destroyed from the business unit, you should check that there are no outstanding reasons to retain the records due for destruction by ensuring you have appropriate internal authorisation or approval processes in place.

If the approved form is not returned within one week, ARMS sends a follow-up notice. ARMS will not destroy records until written confirmation has been received, or until new disposition arrangements are made with your business unit. If you agree, ARMS signs the form to finalize the destruction. ARMS is therefore responsible for retaining the destruction documentation.

Destroying Records

Record destruction must be:

- Irreversible
- Secure and confidential
- Environmentally friendly

Irreversible

Destruction of records should be irreversible so that there is no reasonable risk of the information being recovered again. The more sensitive the information being destroyed, the more certain you must be of the irreversibility of the destruction as failure to ensure total destruction may lead to the unauthorized release of sensitive information.

Information Box

"A number of cases have been reported in the media where records have been found 'unearthed' in local garbage tips after they had been buried, or left in cabinets that had been sold. Records have also been found on the hard drives of computers that have been sold. Such occurrences are very bad publicity for your department and the United Nations as a whole."

ARMS' Guideline on Records Destruction

Environmentally Friendly

Records should be destroyed in as an environmentally friendly manner as possible. All media should be recycled whenever possible, provided you are confident that the data and information has been erased.

Secure and Confidential

Even during the destruction process, you should handle records with the same level of security that was maintained during their life. Ideally, destruction of records should be supervised by an officer of the United Nations or by an authorised agent if destruction has been contracted out.

Methods of Destruction

There are a number of approved destruction methods appropriate for the different media on which the records are stored. These methods are outlined below.

Paper records

Paper records should be shredded or pulped. When shredding records you should ensure that the shredding gauge is as fine as possible. Particularly sensitive documents may need to be cross-shredded. Pulping paper reduces it to its constituent fibres. If carried out correctly, it is a very secure method of destruction.

Both pulped and shredded paper are easily recycled. If neither of these possibilities is available, paper may be burned but this is not environmentally friendly so should be used only as the last resort.

Burying records in landfill is not acceptable as the process is reversible.

Electronic and Magnetic Media

Although electronic and magnetic media often seems very fragile and vulnerable it can also survive and be accessible under very adverse conditions. It is therefore very important to ensure that effective methods are used to erase and recycle or destroy records on these modern media. It is not sufficient to just delete files from electronic media because all you are deleting is the path and any able technician should be able to find the data without it.

Do not forget that backup copies of records also need to be destroyed (including security copies of vital records) at the same time as the masters/working copies. You should consult ARMS and/or ITSD for assistance in destroying electronic and magnetic media.

Magnetic Media

Records stored on magnetic media should be "bulk erased" (by subjecting them to a strong magnetic field) and then reformatted to ensure the data/information cannot be retrieved. The media can then be reused.

Optical Media

Records held on optical media can be destroyed by cutting, crushing, or other physical means of destruction. Never manually snap a disk because of the danger of flying shards. Rewritable optical disks should be reformatted before being disposed of or re-used. Microwaving can be used to destroy optical media but it is only useful for very small quantities. Care must be taken with microwaving due to fumes produced as well as possible harm to the microwave oven. Burning optical media is not recommended as it is not environmentally friendly and produces toxic fumes.

Hard drives

Hard drives of personal computers and servers must be reformatted before computers are disposed of. If in any doubt, the hard drives should be physically destroyed.

Non-Electronic and non-paper media

Videos, cinematographic film and microforms (microfilm/ fiche/ aperture cards/ x-rays) can be destroyed by shredding, cutting, crushing or chemical recycling.

Using a Contractor to Destroy Records

It is not always cost-effective or practical for either ARMS staff or your business unit to destroy records in-house. It is permissible to engage a contractor to destroy records provided the process is supervised and follows the documentation procedures outlined in this section of the Toolkit. Be sure that the contract specifies:

- Suitably secure transport for the records
- That records are destroyed immediately on receipt at the contractors' premises (or at least that the contractor can guarantee their security if this is not possible)
- Acceptable methods of destruction

Responsibilities

Whilst contractors can be engaged to destroy records, it is the responsibility of the business unit to ensure that destruction occurs in accordance with the approved methods of destruction, including protecting sensitive information up until the point of irreversible destruction. Make sure you know what method of destruction your contractor is using.

Transport of records

The contractor can collect records from your office for destruction, or you can deliver the records to them. A closed truck should be used whenever possible. However, if there is no alternative and the contractor can only provide an open truck, ensure that the load is secured by a cover. Sensitive and confidential records should only be conveyed in a closed and locked vehicle.

Documentation

Always insist on a certificate of destruction. If records that were supposed to be destroyed are subsequently found, the certificate is evidence that the contractor was at fault, not your business unit. You may also want to request that the certificate of destruction includes the method used.

Destroying Sensitive Information

There are different types of sensitive information which require particular care in handling and destruction. As noted above, all these should be kept secure from unauthorised access at all times prior to destruction.

Extra care should be given to records containing sensitive personal information. You must have good security in place at all times prior to destruction to ensure the information is safeguarded against loss, unauthorised access, use or disclosure. You should transport the records in lockable containers and/or in totally enclosed and lockable vehicles. They should be destroyed in the presence of an officer of your business unit. For extra security, sensitive paper records may also be shredded in-house before being sent for pulping.

Particular attention should be paid to digital records that contain sensitive information and which need to be destroyed. You are strongly advised to collaborate with CITS and the Risk Management and Quality Assurance Section of ITSD to ensure best practice destruction of digital records.

Personal information

Some business units collect a great deal of information about individuals, and much of this information is quite sensitive, for example investigational, health and welfare records. Even records relating to the licensing of drivers, professions, trades, and commercial activities may contain personal information that could be sensitive. All personal information must be managed in accordance with the requirements of the United Nations Information Security Principles.

Personnel files are a prime example of records containing personal information that have strict access/security restrictions while the records are active. This level of security should be maintained throughout the entire life of these records including during the destruction process.

Financial or commercially sensitive information

Records may contain information of a commercially sensitive nature. Examples include files containing information on a business unit's financial position, tender bids from external companies, and any information on other organisations that may give an unfair financial advantage to a third party.

Information given in confidence

Records may contain information that is given on condition that the information is not released. Examples include personal information and financial information, information given by government agencies (foreign governments, interstate/federal bodies) and information from any source where the provider specifies that it is given in confidence.

Information relating to an investigation

Records relating to an investigation, usually into malpractice or criminal activity, may contain sensitive information. With such records, it is important to ensure that sensitive information is not released through inadequate or inappropriate destruction techniques.

Information posing a security risk

Records may contain information dealing with high security risk activities and premises. Examples of such records are plans of buildings, security plans, procedures for the delivery of large amounts of money, and security arrangements for movements of VIPs.

When the Destruction Date and/or Action needs to be Changed

There can be sound reasons for postponing destruction or even changing the action from destruction to permanent retention. These reasons will have been articulated in the procedures your business unit has in place for ensuring that there is no continuing reason to retain the records. If at this or any other time you realize you need to alter a retention action and/or period the records management officer can do so by completing the RMS 49 Request for Records Disposition Authorization form. ARMS will agree to such a request as long as it can be justified on the basis of financial or legal accountability/responsibility, or on clear programme needs.

The form requires you to give details of the responsible official, their title and your unit, section, office/division and department. You or the appropriate member of the team should then sign and date the form to certify authorization to act for your office on records disposition matters. You will then need to give the series description and your proposed new disposition (for example that you want to retain the records for an additional 2 years). You should also give the existing disposition authorization, which might be a retention schedule or a record plan. The final piece of information to fill in is the justification for changing the agreed retention date and/or action, for example:

"Due to a recent increase in protracted negotiations between the United Nations and Member States, the Secretariat office charged with settling claims has proposed that the three-year retention period currently applicable to related financial records be extended by three years, for a total retention period of six years"

UNITED NATIONS Destruction Form (2 pages)

From: Responsible Official:

Title:

Unit:

Section:

Office/Division:

Department:

Accession number: **Accession date:**

Retention Schedule Number	**Details of records (give description of each record series, including system of arrangement, and attach/ insert a detailed list if available)**	**Quantity (linear feet or number of boxes)**

Covering dates: **Security level:**

Current disposition: **Schedule for disposal date** **Current location**

Destruction Authorisation **(name, signature, date)**	**Business unit:** **Chief, Archives/Registry & Mail/Pouch Unit:**		
FINAL DESTRUCTION CHECK (both boxes must be ticked):	☐ **Retention schedule states destroy permitted** ☐ **Necessary authorisation obtained from department**		
Records have been destroyed	☐	**Date of destruction:**	
Backups have been destroyed (attach details)	☐	**Date of destruction:**	
Proof of destruction attached **Method of destruction:**	☐ ☐ **pulped** ☐ **shredded** ☐ **burnt** ☐ **data erasure**		

Example of an Accession Control Form (2 pages)

United Nations Archives and Records Management Section

ACCESSION CONTROL

Retain this form and the associated file list with your active records to facilitate servicing reference requests. To request records, contact the Reference Desk by telephone at 3.8681/3.8682, by fax at 3.8686 or by Email to current reference staff

Accession Number :	***2004/0066***
Accession Date :	***27/04/2004 at 10:02 AM***
Office of Origin :	***Travel and Transportation Service***
	dm ocss fcsd tts tos
Responsible Official :	***Toshio MIKAMI***
Phone/Ext. Number :	***3-6304***
Room Number :	***S-2012A***
Series Description :	***Records relating to shipment of staff members' household goods and personal effects***
Earliest Date :	***01/01/2002***
Latest Date :	***31/12/2002***
Security Level :	***Unclassified***
Retention Schedule Number :	***RESC03c***
Other Source of Retention :	***n/a***
Current Disposition :	***Archived (Interim)***

Schedule for Disposal Date : ***31/12/2005***

Location : ***Q400-R022-SU14***

Linear Feet : ***39***

Disposition Action : ***Disposal Approval*** ***30/12/2005 at 9 Bridget SISK***

Accession Approval ***30/04/2004 at 9 Ernesto GERONIMO***

DISPOSAL

Office of Origin Approval :

Signature :

For Name, Title and Date, please print clearly

Name : ....

Title : ....

Date : ....

Archives and Records Centre Approval :

Signature :

Name : ....

Title : ....

Date : ....

Method of Disposal : ....

Disposal Date : ....

UN – ARMS United Nations - Room FF-109, New York, NY 10017

RMS.33 (12-96)

☑ Checklist

Records Destruction

- ☐ The records are authorized for destruction under a relevant and current records retention schedule
- ☐ The organisation no longer requires the records
- ☐ The records are not the subject of a current or pending investigation or access request
- ☐ Internal authorisation has been obtained
- ☐ The records have no special security requirements

  OR

  The records have high security level and locked bins and/or in-house shredding are required for security destruction
- ☐ An appropriate service provider has been contacted
- ☐ A covered van/truck has been specified for records removal
- ☐ The service provider has been asked to supply certificate of destruction
- ☐ The agreement specifies that records are to be destroyed on day of collection
- ☐ A certificate has been received by your business unit
- ☐ The records have been destroyed and details of destruction are documented in your business unit's records system

Other Relevant Toolkit Sections

- Section 6 – Managing Sensitive Information
- Section 12 – Managing Records in a Mission Records Storage Facility

Documents

- Field Finance Procedure Guidelines (2001)
- Guideline on Records Destruction (ARMS)
- Peacekeeping Operations Retention Schedule (PORS) (ARMS, 2006)
- Peacekeeping Operations Retention Schedule (PORS) User Handbook (ARMS, 2006)
- United Nations Information Security Principles

Forms

- RMS 33 – accession control form
- RMS 49 – Request for Records Disposition Authorization form

Glossary

Archives: those records which have been selected for permanent preservation because of their administrative, informational, legal and historical value as evidence of official business of the UN. They are a small subset of the UN's records.

Destruction: the act of destroying records, regardless of media, according to appropriate procedures which ensure they are no longer accessible. Also referred to as disposal.

Frequently Asked Questions (FAQs)

What is Destruction?

Destruction is the act of destroying UN records which have reached the end of their retention period. It is carried out according to ARMS policies and procedures to ensure that destruction is properly authorized and documented. This is also referred to as disposal.

What does 'Disposition' Mean?

Disposition is simply a collective term for the various actions and processes to which records are subject over time, such as retention, destruction and transfer to other storage and/or custodians.