

Retention Schedule for ICT Records

United Nations Secretariat ICT Technical Procedure


Ref: INF.05.PROC



Revision History

Serial	Release Description	Release	Release Date	Author(s)
1.	New document	1.0	Sep 2014	Endorsed by ICT Policy Committee
2.	Modify "T=" to "T+"	1.1	Oct 2014	Chair of ICT Policy Committee

Approved By



Atefeh Riazi, ASG/CITO

Date:

Oct, 8, 2014

__ Oct 2014

Retention Schedule for ICT Records United Nations Secretariat ICT Technical Procedure

Section 1

Purpose and Scope

- 1.1 The purpose of this ICT technical procedure is to provide guidance on how to apply retention schedules that have been defined for ICT records, with the ultimate goal of ensuring that ICT records are adequately protected and maintained as well as discarded when no longer needed.
- 1.2 This ICT Technical Procedure covers all ICT records that are system-generated within the United Nations network. It also covers records created by staff members that are used to conduct and support ICT business.
- 1.3 The procedures are in accordance with existing guidance and should not conflict with established policies provided by Archives and Records Management. In case of conflict of retention between existing practice and this Retention Policy, the Business Unit should contact ARMS for resolution.

Section 2

Overview

- 2.1 A *retention schedule* is a timetable that specifies the length of time that records must be retained before disposition. It also defines what disposition action should be taken (destroy or transfer to archives).
- 2.2 Retention schedules are assigned according to the document's useful business life within UN, applicable statutes, regulations and any United Nations policies. Implementing retention schedules within the organization also acknowledges the ongoing challenge and cost of keeping digital records 'alive'- i.e. accessible and readable, beyond their useful value.
- 2.3 Benefits of applying ICT retention schedules include:
 - Enabling offices to standardize the storage and disposition of ICT records;
 - Facilitating the timely destruction and archiving of ICT records;
 - Reducing maintenance and infrastructure costs;
 - Eliminating unnecessary storage costs;
 - Ensuring managed growth of ICT assets;
 - Ensuring transparency to the clients and users as to ICT record policy;
 - Ensuring accountability and consistency as to disposal;
 - Preventing records with no continuing usefulness from slowing down the system;
 - Eliminating any risk of sensitive or personal information falling into the wrong hands.

Section 3

Definitions

3.1 The following definitions shall apply for the purposes of the present procedure:

- (a) *Authorized User*: any staff member who is authorized to use information and communication technology (ICT) resources;
- (b) *ICT service providers*: United Nations Secretariat organizational units that provide ICT services to one or more Secretariat entities;
- (c) *Office of record*: The office of record is the office or administrative unit that has been designated for the maintenance, preservation and disposition of record (official) copies.
- (d) *Record*: any data or information, regardless of form or medium, maintained by the United Nations as evidence of a transaction; A record can be represented in any medium, for example paper, reports, completed forms, data on hard drives, servers, disks, tapes and microfilm;
- (e) *ICT record*: a record relevant for ICT management;
- (f) *IT Equipment*: includes desktop and laptop computers, as well as servers, firewalls, etc.
- (g) *Aggregation*: accumulated or collected records that are organized into groupings or series.

Section 4

Overall responsibility and accountability

- 4.1 ICT Service Providers and Business Units are responsible for implementing this ICT Technical Procedure.
- 4.2 ICT Service Providers in OAHs, Regional Commissions, DFS/ICTD and OICT must follow the Information and Communication Technology Records Retention Policy for UN Secretariat ICT Service Providers, attached in Annex 2.
- 4.3 All other Business Units in which ICT services are being provided, must follow the Information and Communication Records Retention Policy for UN Secretariat Offices other than ICT Service Providers, attached in Annex 1

Section 5

Elements of retention schedules

5.1 Retention schedules contain the following elements

- Record series
- Retention period
- Trigger
- Aggregation
- Disposition

5.2 Record Series is a group of related documents which are normally used and filed as a unit, and are evaluated as a unit for retention scheduling purposes.

5.3 Retention period gives the total time the records are to be retained, regardless of their location. Retention periods are generally expressed as a code (called a ‘trigger’) plus a number. The number is the number of years the records are to be kept after the occurrence of the event or ‘trigger’ indicated by the code. For example, in a retention schedule of ‘C+2’, ‘C’ is the trigger that means ‘Current year’ and ‘2’ means 2 years after the trigger occurred. In that example, if the current year is 2013, records covered in that record series should be retained for 2014 and 2015.

5.4 Trigger: a trigger is an event from which a retention period is calculated. Triggers are shown in the retention schedules by codes, as follows

Trigger Code	Description	
C	Current year	Maintain record until the end of the current year.
T	Terminated	Retain until termination, expiration or completion; ‘T’ must be defined for each record series

Triggers can be known from the beginning of a record series lifecycle, or not. The triggers that are known from the start are ‘C’, because they’re based on a year that is known. The triggers that start with ‘T’ depend on someone to provide a date.¹

¹ The record series ‘Capacity Usage Reports’ has a retention of C+10. The trigger ‘C’ means current year and the retention period is 10 years. In this case no further action by the owner of the record is needed to apply retention. The record series ‘Network Service Work Orders’ has a retention of T+2. The trigger ‘T’ in this case means ‘completion of the work order’ and the retention period is 2 years after the work order is completed. The owner of the record needs to indicate that the event in question has been completed, i.e. usually by ‘closing’ the annual work order folder.

5.5 Aggregation: aggregation indicates if retention schedules for records should be managed individually (by document) or in groups (by folders) for the purposes of aging and disposition. Depending on the particular case, it is typically considered best practice to manage records by folders.

5.6 Disposition: disposition indicates what happens when records have passed their retention periods. The options are Destroy or Keep Permanently.

Section 6

Ongoing Revisions

6.1 This ICT Technical Procedure must be reviewed by the ICT Policy Committee on an ongoing basis.

6.2 Each department should review its retention schedule annually

- Records now being received or generated in the department which are not listed on the retention schedules, should be added;
- Records which are no longer received, generated or maintained in the office, should be identified for deletion from the retention schedule;
- Acquisition or adaptation of new technologies;
- Changes to retention periods should be noted;
- The status of a record as vital (disaster recovery), notes regarding the record series, and changes in the office of record should also be reviewed closely and changed if necessary;
- The proposed revisions will be reviewed by OICT, ARMS, the UN Office of Legal Affairs, and Internal Audit Division of OIOS, as appropriate.

Section 7

Additional References

- 1- ARMS User Guide to Retention Schedule Implementation
https://archives.un.org/sites/archives.un.org/files/files/Policy_Guideline/Guideline_retention%20schedule%20implementation.pdf
- 2- ARMS - Principles of Records Destruction
https://archives.un.org/sites/archives.un.org/files/files/Policy_Guideline/Records_Destruction_Guideline.pdf
- 3- ST/SGB/2004/15 - Use of Information and Communication Technology Resources and Data
- 4- ST/SGB/2007/5 - Record-keeping and the Management of United Nations Archives

Annex 1: Information and Communication Technology Records Retention Schedule - Retention Policy for UN Secretariat Business Unites other than ICT Records Providers

Retention code	Records series title	Description	Disposition and Retention Notes	Office of Record
BU_ICT-01	Project Management Documents for ICT Projects	Copies of Project management records, project briefs, business cases, status reports, feasibility study reports documenting the analysis of information management problems to determine effective operational, economical and technical solutions; also includes data collection material such as: interview notes, questionnaires, computer printouts, requirements analysis documents, and related correspondence. Assessments conducted following the completion of each IT project that address operational problems (whether the project met proposed objectives, was completed within the anticipated time and budgetary constraints, and achieved the proposed benefits). Includes: surveys, gap analysis checklists, third party recommendations, and auditor comments.	T+5, Destroy, T = completion of the project or end of life of application or system	ICT service provider
BU_ICT-02	System Design Documents	Copies of documents that examine the IT problem and the creation of its solution. Includes system architectural diagrams, database design	T+5, Destroy, T = completion of the project or end of life of application or system	ICT service provider
BU_ICT-03	Maintenance and configuration management	Copies of Configuration Management Database and configuration management related documents. Change requests and other change management records.	T+5, Destroy, T = completion of the project or end of life of application or system	ICT service provider

BU_ICT-04	Delivery	Copies of Setup instructions, deployment procedures and manuals/instructions	T+5, Destroy, T = completion of the project or end of life of application or system	ICT service provider
BU_ICT-05	Change Management	Communications strategy, Training strategy and stakeholder management strategy, change strategy	T+5, Destroy, T = completion of the project or end of life of application or system	ICT service provider
BU_ICT-06	Testing Data and Documents	Copies of user testing processes created prior to implementation of a new or revised application. Contains a sample of every category of valid data as well as many invalid conditions as possible and includes: test programs/scripts with their results, instructions, routines, validity checking and verification data, user acceptance tests, and other test documentation.	T+5, Destroy, T = completion of the project or end of life of application or system	ICT service provider
BU_ICT-07	(User) Program Documentation & Training Materials	Copies of User manuals or training materials for the systems or applications.	T+5, Destroy, T = completion of the project or end of life of application or system	ICT service provider
BU_ICT-08	Database and Meta data documentation	Copies of Meta data definitions, data structures, file layout and reports concerning the development and/or modification of an automated system as well as the metadata for access, retrieval, manipulation and interpretation of data in this automated system.	T+5, Destroy, T = completion of the project or end of life of application or system	ICT service provider

Clients Support / Service Provision Records: retention is 5 years after delivery of service or users name is removed from systems (T+5).
 Destroy

BU_ICT-09	IT Access Authorizations	Records documenting the issuance of passwords, personal identity management, VPN requests, user acknowledgements and change requests about access authorizations, remote access agreements, requests for blocked internet sites, temporary/permanent firewall access requests and profiles, maintenance and closure of user accounts.	T+5, T= delivery of service or users name is removed from systems	Business Unit
BU_ICT-10	User requests for IT services and help desk logs	Records used to document user requests to recover data from backup or archives stores and actions taken; records documenting the request for technical assistance/services and responses for these requests as well as to collect information on the use of computer equipment to compile periodic statistics and for reference for planning, management analysis and other administrative purposes.	T+5, T= delivery of service or users name is removed from systems	Business Unit
Infrastructure Management Records: If delegated authority refer to OICT Retention Policy OICT15-OICT23				
Information Security Records: retention is 5 years after the incident and destroy. T+5, Destroy				
BU_ICT-11	Information Security Incident	Reported or detected information security incidents. Reports, logs, extracts and compilations of data related to security incidents, misuse of ICT systems and actions taken.	T+5, Destroy, T= date of incident	ICT service provider
BU_ICT-12	Disaster Prep. and Recovery Planning Docs	Business impact analysis documents, Disaster recovery plans and procedures, business continuity plans, contingency plans and any referenced document related to Disaster preparedness and recovery.	T+5, Destroy, T= date of incident	Business Continuity Section
BU_ICT-13	Disaster Incident reports	Reports documenting disaster incidents, their cause, effects, costs, action taken, any related actions taken to limit future risks.	T+5, Destroy, T= date of incident	ICT service provider

ICT Governance records: retention is 10 years (C+10) after meeting or superseded Policy, except the Governance, Policies, Standards, Procedures which are kept Permanently (P, A).				
BU_ICT-14	Meeting documents of ICT governance bodies	Copies of Records of minutes of governance bodies and attachments of minutes.	C+10, Destroy, C= year of meeting	ICT service provider
BU_ICT-15	Governance Policies, Standards, Procedures	Copies of ICT related Strategies, Policies, Standards, Procedures, guidelines, plans etc.	Keep Permanently	ICT service provider
IT Asset Management: retention is 3 years after disposal of the asset or inventory superseded. T+3, Destroy				
BU_ICT-16	Data System Equipment information and Support Files	Copies of Information about the hardware, software and other products and their vendors such as purchase orders, warranties, service contracts, service reports, service histories and correspondence.	T+3, Destroy, T= disposal of asset	ICT service provider
BU_ICT-17	Hardware Inventory	Records documenting common hardware inventory such as servers, routers, switches per organizational unit	T+3, Destroy, T= disposal of asset	ICT service provider

Retention Codes (Triggers)

C = Current Year

T = Termination, Settlement or Completion

Annex 2: Information and Communication Technology Record Retention Schedule - Retention Policy for UN Secretariat ICT Service Providers.

Application Development and Implementation Records: retention is 10 years after completion of the project or end of life of application or system (T+10). Exceptions are IT projects above \$200,000 are kept permanently (P)				
Retention code	Records series title	Description	Disposition and Retention Notes	Office of Record
OICT-01	Project Management Documents for ICT Projects over \$200,000	Project management records, project briefs, business cases, status reports, feasibility study reports documenting the analysis of information management problems to determine effective operational, economical and technical solutions; also includes data collection material such as: interview notes, questionnaires, computer printouts, requirements analysis documents, and related correspondence. Assessments conducted following the completion of each IT project that address operational problems (whether the project met proposed objectives, was completed within the anticipated time and budgetary constraints, and achieved the proposed benefits). Includes: surveys, gap analysis checklists, third party recommendations, and auditor comments.	Keep permanently	ICT service provider
OICT-02	Project Management Documents for ICT Projects Under \$200,000	Project management records, project briefs, business cases, status reports, feasibility study reports documenting the analysis of information management problems to determine effective operational, economical and technical solutions; also includes data collection material such as: interview notes, questionnaires, computer printouts, requirements analysis documents, and related correspondence. Assessments conducted following the completion of each IT project that address operational problems (whether the project met proposed objectives, was completed within the anticipated time and budgetary constraints, and achieved the proposed benefits). Includes: surveys, gap analysis checklists, third party recommendations, and auditor comments.	T+10, Destroy, T = completion of the project or end of life of application or system	ICT service provider

OICT-03	System Design Documents	This records series documents the examination of an IT problem and the creation of its solution. Includes system architectural diagrams, database design, .	T+10, Destroy, T = completion of the project or end of life of application or system	ICT service provider
OICT-04	Maintenance and configuration management	Configuration Management Database and configuration management related documents. Change requests and other change management records.	T+10, Destroy, T = completion of the project or end of life of application or system	ICT service provider
OICT-05	Delivery	Setup instructions, deployment procedures and manuals/instructions	T+10, Destroy, T = completion of the project or end of life of application or system	ICT service provider
OICT-06	Change Management	Communications strategy, Training strategy and stake holder management strategy, change strategy	T+10, Destroy, T = completion of the project or end of life of application or system	ICT service provider
OICT-07	Testing Data and Documents	These file sets document programmer and user testing processes created prior to implementation of a new or revised application. Contains a sample of every category of valid data as well as many invalid conditions as possible and includes: test programs/scripts with their results, instructions, routines, validity checking and verification data, user acceptance tests, and other test documentation.	T+10, Destroy, T = completion of the project or end of life of application or system	ICT service provider

OICT-08	Program Source Code & Programmer Documentation	This records series consists of programming statements and instructions that are written by a programmer, and convertible into machine language by compilers, assemblers or interpreters; and, other documentation the programmer utilizes for application implementation. May also include: data systems/file specifications, codebooks, file layouts, and output specifications.	T+10, Destroy, T = completion of the project or end of life of application or system	ICT service provider
OICT-09	(User) Program Documentation & Training Materials	User manuals or training materials for the systems or applications.	T+10, Destroy, T = completion of the project or end of life of application or system	ICT service provider
OICT-10	Database and Meta data documentation, Projects over \$200,000	Meta data definitions, data structures, file layout and reports concerning the development and/or modification of an automated system as well as the metadata for access, retrieval, manipulation and interpretation of data in this automated system.	Keep Database documentation Permanently for projects over \$200,000	ICT service provider
OICT-11	Database and Meta data documentation, projects under \$200,000	Meta data definitions, data structures, file layout and reports concerning the development and/or modification of an automated system as well as the metadata for access, retrieval, manipulation and interpretation of data in this automated system.	T+10, Destroy, T = completion of the project or end of life of application or system	ICT service provider
Clients Support / Service Provision Records: retention is 5 years after delivery of service or users name is removed from systems (T+5), except Communication Records which has a 3 year retention (T+3) Destroy.				
OICT-12	IT Access Authorizations	Records documenting the issuance of passwords, personal identity management, VPN requests, user acknowledgements and change requests about access authorizations, remote access agreements, requests for blocked internet sites, temporary/permanent firewall access requests and profiles, maintenance and closure of user accounts.	C+5, Destroy, C= date of delivery of service or users name is removed from systems	ICT service provider

OICT-13	User requests for IT services and help desk logs	Records used to document user requests to recover data from backup or archives stores and actions taken; records documenting the request for technical assistance/services and responses for these requests as well as to collect information on the use of computer equipment to compile periodic statistics and for reference for planning, management analysis and other administrative purposes.	C+5, Destroy, C= date of delivery of service or users name is removed from systems	ICT service provider
OICT-14	Communication records	Telephone call logs, faxes logs, mobile logs, code cables logs	T+3, Destroy, T = completion of applicable review and verification procedures, or after any litigation, claim, audit or other official action involving the records has been completed.	ICT service provider
Infrastructure Management Records: retention varies see below				
OICT-15	System Backup – recovery files	Copies of software, Database Management System configuration files, directories and other records needed to restore a system.	T+5, Destroy, T = replacement of previous backup copy	ICT service provider
OICT-16	Storage System Records	List of backup tapes, disks and/or storage control records.	T+5, Destroy, T=previous version superseded	ICT service provider

OICT-17	Network and Internet Usage Logs	Monitor network access including Service Logs, Mail server logs, Website logs, FTP logs, Telnet logs, Firewall and proxy logs, Application logs, Log-in files, Data entry logs as well as related reports such as: Authentication and Authorization Reports, Systems and Data Change Reports, Network Activity Reports, Resource Access Reports, Malware Activity Reports and Failure and Critical Error Reports	C+2, Destroy, C= Current Year	ICT service provider
OICT-18	Email Backup	Backup is NOT meant for archiving but for the disaster recovery of the email system or for accidental deletion within a two week period. After two weeks the backup data is cloned from the virtual tape into the physical tape library and shipped to external site for storage. Email backups are kept 10 years on tape at a remote location.	C+10, Destroy, C=Current Year	ICT service provider
OICT-19	Data Backup Media	This retention policy is the default policy, applied to virtually all backups except the email backups. Notably, the policy is used to back up the "shared drives" and NFS file systems of the Celera filers (data movers) using Network Data Management Protocol technology	C+3, Destroy, C=Current Year	ICT service provider
OICT-20	Capacity Usage Reports	Capacity usage reports/files for cost recovery, benefit analysis and future planning purposes.	C+10, Destroy, C=Current Year	ICT service provider
OICT-21	Network Implementation Project	Records used to plan and implement a network including reports, justifications, diagrams, etc.	Keep permanently (P)	ICT service provider
OICT-22	Network / Circuit Installation and Service	Work orders, correspondence, work schedules.	T+2 , Destroy, T = completion of work order	ICT service provider
OICT-23	System Architecture documents and Wiring schemas	Building/circuit diagrams and other records documenting the location of wiring and the design of the overall network environment.	S+10, Destroy, S= superseded Architecture or wiring schemas	ICT service provider

Information Security Records: retention is 5 years after the incident. Exception is disaster incident report which is kept permanently				
OICT-24	Information Security Incident	Reported or detected information security incidents. Reports, logs, extracts and compilations of data related to security incidents, misuse of ICT systems and actions taken.	T+5, Destroy, T = incident	ICT service provider
OICT-25	Disaster Prep. and Recovery Planning Docs	Business impact analysis documents, Disaster recovery plans and procedures, business continuity plans, contingency plans and any referenced document related to Disaster preparedness and recovery.	T+5, Destroy, T = incident	ICT service provider
OICT-26	IT Asset Audit Records	Records documenting the routine monitoring and testing of the operations of ICT systems and actions taken to rectify problems and optimise performance. These can be analysis reports, review reports, risk assessment reports or other audit documents regarding the maintenance and security of the IT asset.	T+5, Destroy, T = incident	ICT service provider
OICT-27	Disaster Incident reports	Reports documenting disaster incidents, their cause, effects, costs, action taken, any related actions taken to limit future risks.	Keep permanently	ICT service provider
ICT Governance records: retention is permanent				
OICT-28	Meeting documents of ICT governance bodies	Records of minutes of governance bodies and attachments of minutes.	Keep permanently	ICT service provider
OICT-29	Governance Policies, Standards, Procedures	ICT related Strategies, Policies, Standards, Procedures, guidelines, plans etc.	Keep permanently	ICT service provider
IT Asset Management: retention is 5 years after disposal of asset or inventory superseded.				

OICT-30	Data System Equipment information and Support Files	Information about the hardware, software and other products and their vendors such as purchase orders, warranties, service contracts, service reports, service histories and correspondence.	T+5, Destroy, T = disposal of asset or inventory superseded	ICT service provider
OICT-31	Asset Inventories	Records documenting the assignment of a specific computer or mobile ICT systems to an individual	T+5, Destroy, T = disposal of asset or inventory superseded	ICT service provider
OICT-32	Hardware Inventory	Records documenting common hardware inventory such as servers, routers, switches per organizational unit	T+5, Destroy, T = disposal of asset or inventory superseded	ICT service provider
OICT-33	Software Inventory	Records documenting specific computer or mobile ICT systems to organizational unit	T+5, Destroy, T = disposal of asset or inventory superseded	ICT service provider

Retention Codes (Triggers)

C = Current Year

T = Termination, Settlement or Completion

--- End of Document ---