CAYMAN ISLANDS
NATIONAL ARCHIVE
CAYMAN ISLANDS GOVERNMENT

Disposal Authorisation
for
Information and Technology Management Records

Administrative Schedule No. 4

July 2014, Revised April 2023

CAYMAN ISLANDS
NATIONAL ARCHIVE
CAYMAN ISLANDS GOVERNMENT

AUTHORISATION FOR THE COMMENCEMENT OF THIS SCHEDULE

Issued under the National Archive and Public Records Act (2015 Revision)

Authorisation:-

Under Section 8 of the National Archive and Public Records Act (2015 Revision), I hereby approve relevant public agencies (as defined under Section 2(1) of the National Archive and Public Records Act (2015 Revision) to administer the disposal of public records in accordance with the prescribed retention periods set out herein.

Franz I. Manderson
Deputy Governor

Date: August 25, 2023

1. Introduction

The National Archive and Public Records Act (2015 Revision) provides the regulatory framework to support the disposal of government's informational assets past their retention periods. Approval for the destruction of public records is stipulated in accordance with Section 6(2) b. This Schedule sets retention periods for the information and technology management administrative records of all public agencies. Disposal of public records involves destruction, acquisition by the National Archive, and records transferred to the custody and ownership of another agency.

2. Legislative Framework

This Schedule is issued under Section 8 of the National Archive and Public Records Act (2015 Revision) and is a requirement for every public agency as defined under Section 2(1) of this Act. Evidentiary backing within practice for establishing a sound records and information management infrastructure is supported by the following legislation:-

- The Cayman Islands Constitutional Order 2009
- Public Service Management Act (2018 Revision)
- Public Service Management Act – Personnel Regulations (2022 Revision)
- Public Management and Finance Act (2020 Revision)
- Public Management and Finance Act – Financial Regulations (2022 Revision)
- Freedom of Information Act (2021 Revision)
- Freedom of Information (General) Regulations (2021 Revision)
- Data Protection Act (2021 Revision)
- The Data Protection Regulations, 2018
- Evidence Act (2021 Revision)
- Electronic Transactions Act (2003 Revision)
- Limitation Act (1996 Revision).

3. Exclusions

This Schedule does not cover the destruction of public records:-

a) If records are deemed to have intrinsic or archival value regardless of its original format or media or records that will be held permanently within agencies.
b) If there is a government policy or directive not to destroy public records.
c) If public agencies are reasonably aware records may be required for judicial matters or audits.
d) If records are subject to access inquiries or appeals under the Freedom of Information Act.
e) If the records are subject to the provisions of the Data Protection Act, including but not limited to the following: subject access requests, appeals, stop/restrict processing notices, complaints, and personal data breaches.

f) If the records relate to an operational function of a public agency. Such agencies may find the guidance informative, however, their records should be included in the operational disposal authority for the relevant public agency.
g) If the Cayman Islands National Archive has issued a standard prohibiting the destruction of specific records required for incorporation into the Historical Collection for long-term preservation.

ITM	INFORMATION AND TECHNOLOGY MANAGEMENT	
ITM/AUD	**AUDITING** Officially checking quality assurance and operational records to examine whether information technology management activities are being accurately documented in accordance with legislation, agreed standards, regulations, best practices, procedures and plans. Includes compliance, recordkeeping system, quality assurance and security audits/risk assessments.	
ITM/AUD/01	**Internal and external compliance audits** Conducted within Government or by private parties on compliance with information technology and telecommunications standards, such as ISO 9000 series. Includes correspondence, arrangements, audit forms, final reports and feedback. Also documentation of routine inspections of ITM assets, e.g. recordkeeping practices, software related surveys, system statistics, etc.	**Review by agency 7 years after final report completed/last action.**
ITM/DSL	**CONTROL – MAINTENANCE & DISPOSAL** Activities related to record centre operations and other secure and controlled storage for public records and archives. Includes arrangements for physical storage. Excludes: security (use ITM/POL/02), finance related records and documentation (see FM/ACQ) and disposal of hardware (use FM/ACQ/02).	
ITM/DSL/01	**Offsite storage** Correspondence relating to maintenance and management.	**Destroy 6 years after contract expired/terminated.**
ITM/DSL/02	**Retrieval of records** Includes copies of delivery lists for the retrieval and return of records to/from the Government Records Centre and records relating to retrieval/return to/from other offsite storage.	**Destroy 2 years after records were disposed.**
ITM/DSL/03	**Location lists** Documenting the location of records stored on and offsite.	**Destroy 2 years after list superseded.**
ITM/DSL/04	**Transfer of archival records** Documenting the transfer of ownership of records, identified as archival in disposal schedules, from entities defined under the *National Archive and Public Records Act (2015Revision)* to the National Archive.	**Permanently held in agency.**
ITM/DSL/05	**Transfer of records to/from another entity** Records documenting transfer of custody, control or ownership of agency through restructuring or privatisation.	
ITM/DSL/06	**Certificates of destruction** Includes Proof of Destruction forms.	
ITM/DSL/07	**Review lists** List of records that are on review for disposal (i.e. destruction or transfer to CINA).	**Destroy 5 years after action completed.**
ITM/DSL/08	**Approved file plan and disposal schedules**	**Permanently held in agency.**
ITM/DSL/09	**File plan and disposal schedule development**	**Destroy 10 years after last action.**
ITM/DSL/10	**Recordkeeping advice and guidance**	**Destroy 5 years after last action.**

ITM/FOI	**FREEDOM OF INFORMATION** Managing applications/requests, appeals and enquiries received under the Freedom of Information (FOI) Act or related to information disclosure. Includes plans and policy records in relation to the agency's implementation of the FOI Act and the agency's obligations under it; records demonstrating compliance with the FOIA; and records relating to decisions about releasing, withholding or redacting records as a result of FOI requests. Excludes: records of financial transactions, e.g. payments of fees (use FM/ACC/02).	
ITM/FOI/01	**Implementation planning and compliance** Documenting how to fulfil the agency's legal obligations under the FOI Act, e.g. project plans, procedures for handling requests or for proactive publication, appointment of Information Managers, staff training. Includes monitoring to ensure implementation goes according to schedule and standards are met, and documentation for introduction of new software. Excludes: statistical data (use ITM/FOI/06) and practitioner training (use ITM/FOI/02).	Destroy 3 years after superseded/obsolete.
ITM/FOI/02	**Training, guidance and resources** Supporting documentation and notes in preparation for and as a result of a meeting, training session or resource distribution for Information Managers and other FOI practitioners. Includes records created as a result of general guidance circulated by subject matter experts or by the supervisory authority. Excludes: routine communication and information received from other agencies, e.g. registration confirmation and reminders regarding training (see HR/DEV) and records relating to the processing of a specific FOI request (use ITM/FOI/03) or general inquiry handled by the Information Manager (use ITM/FOI/04).	Destroy 1 year after superseded/last action.
ITM/FOI/03	**Requests and appeals of decisions** Records relating to the processing of FOI requests and subsequent appeals under the FOIA, as well as the monitoring or tracking of requests through all stages. Includes copies of records released, correspondence with applicants, third parties, the supervisory authority, and any other person consulted in relation to the request and/or appeal (e.g. legal counsel and subject-matter experts). Where a request proceeded to internal review, appeal to the supervisory authority, judicial review, and/or any further appeal before the courts, includes records relating to the appeal and its determination as well as monitoring compliance with any decisions and/or orders. All records should be cross-referenced with the original request case file using the assigned FOI reference number. Includes registers, logs and all data contained within any tracking and monitoring system. Last action includes closure of the request in any tracking and monitoring system.	Destroy 3 years after last action if decision/internal review was not appealed. Destroy 7 years after appeal resolved if decision/internal review was appealed to an external authority.
ITM/FOI/04	**General inquiries** Inquiries handled by Information Managers in this official capacity. Includes inquiries from members of the public relating to the FOI Act and requests for information that are handled in the normal course of business and not as formal applications under the FOI Act. Excludes: media inquiries and responses about agency initiatives, events and programmes (use COM/MDA/07).	Destroy 3 years after last action on inquiry.

ITM/FOI/05	**Complaints** Complaints regarding the performance of the agency relating to information disclosure and the processing of requests for records under the FOIA. Includes the original complaint and all records relating to the investigation and determination of the complaint by the agency or any other person, including the supervisory authority. Includes records relating to measures taken to monitor compliance with any recommendations or orders made as a result of the complaint. Includes registers, logs and all data contained within any tracking and monitoring system.	Destroy 7 years after complaint closed.
ITM/FOI/06	**Reports** Internal and external reports on the operation of the FOI Act within the agency, including reports provided to auditors and other competent authorities and reports submitted to the supervisory authority.	Destroy 1 year after report submitted.
ITM/FOI/07	**Publication Schemes** Documents created to comply with the Code of Practice on Publishing issued under the FOI Act. Includes records relating to the proactive publication of an agency's information which is readily available to the public without the need for specific written requests.	Destroy 2 years after superseded/obsolete. Note: send a copy to the National Archive prior to destruction.
ITM/FOI/08	**Disclosure Logs** List of FOI requests (which may be summarised) and details of their outcomes. May include copies of records that were released, as well as redacted copies of decision letters that were sent to applicants. Records disclosed in response to an FOI request (ITM/FOI/03) that are public records may be included in the Disclosure Log beyond their minimum retention period if deemed to be in the public interest.	Permanently held in public agency.
ITM/FOI/09	**Training for public officials (agency internal training)** Information Managers and other public officials providing opportunities for internal training on FOI, access to information and directly related matters. Includes developing and delivering internal courses and workshops, arranging attendance at external courses and retreats, and course evaluations. Excludes: certificates and other records confirming completion of training courses by staff (use HRA/STA/01).	Destroy 2 years after course delivered.
ITM/PDP	**PRIVACY AND DATA PROTECTION** Managing complaints, requests, notices and orders received under or pursuant to the Data Protection Act (DPA) and other privacy legislation. Includes plans and policy records in relation to actions taken by the to comply with the DPA and other privacy legislation and the agency's obligations under it; records demonstrating compliance with the DPA and other privacy legislation; records relating to decisions about releasing, withholding or redacting records as a result of data subject access requests; and records relating to decisions made about the processing of specific personal data as a result of requests or notices from data subjects. Excludes: records of financial transactions, e.g. payments of fees (use FM/ACC/02).	

ITM/PDP/01	**Implementation planning and compliance** Documenting how to fulfil the agency's legal obligations under the DPA and other privacy legislation or policies, e.g. project plans, procedures for handling requests or notices, appointment of Data Protection Leaders, and staff training. Includes monitoring to ensure implementation goes according to schedule and standards are met, and documentation for introduction of new software. Excludes: statistical data (use ITM/PDP/11) and practitioner training (use ITM/PDP/02).	Destroy 3 years after superseded/obsolete.
ITM/PDP/02	**Training, guidance and resources** Supporting documentation and notes in preparation for and as a result of a meeting, training session or resource distribution for Information Managers, Data Protection Leaders and other data protection practitioners. Includes records created as a result of general guidance circulated by subject matter experts or by the supervisory authority. Excludes: routine communication and information received from other agencies, e.g. registration confirmation and reminders regarding training (see HR/DEV), records relating to the processing of or response to a specific general inquiry (use ITM/PDP/06), data subject access request (use ITM/PDP/07), stop/restrict processing notice (use ITM/PDP/08), order regarding inaccurate personal data (use ITM/PDP/09), complaint (use ITM/PDP/10), or security incident (use ITM/PDP/13).	Destroy 1 year after superseded/last action.
ITM/PDP/03	**Data maps and inventories** Includes Records of Processing Activities (RoPAs) and all other methods for documenting the processing of personal data by the agency.	Destroy 7 years after superseded/obsolete.
ITM/PDP/04	**Policies** Policies developed by the agency to comply with the Data Protection Principles, other provisions of the DPA, and any other legislation to which the agency may be subject in relation to privacy and data protection. Includes Data Protection Policies and policies developed in relation to Data Protection Impact Assessments, responses to security incidents and personal data breaches, and the handling of data subject access requests and/or notices relating to the exercise of other individual rights under the DPA.	Destroy 7 years after superseded/obsolete.
ITM/PDP/05	**Privacy Notices** Documents created to provide privacy information to data subjects, including the purposes for processing personal data and how the personal data will be used, categories of personal data processed, sources of personal data, legal bases for processing, applicable retention periods, data subject rights, potential recipients, security measures and international transfers. Includes external privacy notices, employee privacy notices and cookie notices.	Destroy 7 years after superseded/obsolete.

ITM/PDP/06	**General inquiries** Privacy and data protection-related inquiries handled by Information Managers and Data Protection Leaders in this official capacity. Includes inquiries from members of the public relating to the DPA, including requests for the data subject's own personal data that are handled in the normal course of business and not as formal applications under the DPA. Excludes: media inquiries and responses about agency initiatives, events and programmes (use COM/MDA/07).	Destroy 3 years after last action on inquiry.
ITM/PDP/07	**Data subject access requests** Includes correspondence with applicants, third parties, the supervisory authority, and any other person consulted in relation to the request and/or appeal (e.g. legal counsel and subject-matter experts). Where a request proceeded to a complaint to the supervisory authority, judicial review, and any further appeal before the courts, includes records relating to the complaint or appeal and its determination as well as compliance with any decisions and/or orders. All records should be cross-referenced with the original written request. Includes all data contained within any tracking and monitoring system. Excludes: where a data subject access request is treated as a Freedom of Information request (use ITM/FOI/03).	Destroy 3 years after last action if the data subject did not complain to the supervisory authority. Destroy 7 years after complaint resolved if the data subject complained to the supervisory authority.
ITM/PDP/08	**Stop/restrict processing notices** Notices to stop or restrict the processing of personal data, inclusive of automated decision-making processes and ceasing direct marketing activities. Also includes the notice initially received from the data subject, correspondence with the data subject, third parties, the supervisory authority, and any other person consulted in relation to the notice and/or subsequent appeal of or complaint regarding the decision (e.g. legal counsel and subject-matter experts). Where a notice proceeded to a complaint to the supervisory authority, judicial review and any further appeal before the courts, includes records relating to the complaint or appeal and its determination as well as compliance with any decisions and/or orders. All records should be cross-referenced with the original written notice. Includes all data contained within any tracking and monitoring system.	Destroy 7 years after last action.
ITM/PDP/09	**Complaints** Complaints regarding the processing of personal data that (allegedly) has not been or is not being carried out in compliance with the provisions of the DPA or anything required to be done pursuant to the DPA. Includes the original complaint and all records relating to the investigation and determination of the complaint by the agency or any other person, including the supervisory authority. Includes records relating to measures taken to monitor compliance with any recommendations or orders made as a result of the complaint. Includes registers, logs and all data contained within any tracking and monitoring system. Excludes complaints resulting from Data Subject Access Requests (use ITM/PDP/07).	Destroy 7 years after complaint closed.

ITM/PDP/10	**Reports** Internal and external reports on the operation of the DPA within the agency, including reports provided to auditors and other competent authorities and reports submitted to the supervisory authority.	Destroy 1 year after report submitted.
ITM/PDP/11	**Training for public officials (agency internal training)** Data Protection Leaders and other public officials providing opportunities for internal training on privacy, data protection and directly related matters. Includes developing and delivering internal courses and workshops, arranging attendance at external courses and retreats, and course evaluations. Excludes: certificates and other records confirming completion of training courses by staff (use HRA/STA/01).	Destroy 2 years after course delivered.
ITM/PDP/12	**Security incident response and personal data breaches** Includes internal reports of actual or suspected personal data breaches records of investigations into security incidents and personal data breaches, notifications to the supervisory authority and to data subjects, summary of actions taken as a result of breaches, and monitoring of compliance with any recommendations or orders arising from a security incident or personal data breach. Includes registers, logs and all data contained within any tracking and monitoring system.	Destroy 7 years after incident/breach closed.
ITM/PDP/13	**Documentation of personal data sharing and disclosure** Includes Memoranda of Understanding, Terms of Service and other written agreements or records developed to document and/or govern the sharing of personal data between public authorities, the engagement of public authorities as Data Processors, and the disclosure of personal data to a third party. Excludes external vendor contracts (use FM/ACQ/03).	Destroy 7 years after superseded/data sharing ceases.
ITM/PDP/14	**Data Protection Impact Assessments (DPIAs)** Includes correspondence with data subjects, subject matter experts and other stakeholders as the DPIA is being conducted. Where a public authority is required to consult with the supervisory authority, includes all correspondence with the supervisory authority.	Destroy 7 years after superseded/processing ceases.
ITM/IPY	**INTELLECTUAL PROPERTY - COPYRIGHT** Management of agency's intellectual property and use of material held by the agency which is the intellectual property of another party. Includes the administration of crown copyright. Excludes: the administration of payments (see FM/ACC) and policy and procedures (see ITM/POL).	
ITM/IPY/01	**Reproduction requests** Applications received by public agency for permission to reproduce material for which it owns copyright.	**Destroy 7 years after last action.**
ITM/IPY/02	**Applications for use of copyright** Applications made by public agencies to use copyrighted material (including software) owned by another party.	
ITM/IPY/03	**Copyright infringement** Documentation relating to copyright infringement cases.	
ITM/IPY/04	**Copyright declaration forms**	

ITM/LIB	**CONTROL – LIBRARY** Acquiring and maintaining print and electronic documents, official and other publications for reference use by staff. Includes records documenting the library system. Excludes: record surveys (see ITM/RCD/03) and policy and procedures (see ITM/POL).	
ITM/LIB/01	**Catalogues** Includes descriptive records of the Staff Library collection to make materials in the collection more accessible. E.g. indexes, classification schemes and thesauri.	**Destroy once entity no longer exists.**
ITM/LIB/02	**Subscriptions** Includes records of memberships to e-journals/magazines, professional journals, associations and societies.	**Destroy 7 years after expiration/renewal/ cancellation of subscription.**
ITM/PLA	**PLANNING** Discussing and preparing to implement, manage and monitor ITM-related activities. Evaluating needs, setting objectives and designing strategies to achieve proposed outcomes. Excludes **s**oftware development (see ITM/SOF).	
ITM/PLA/01	**Final versions of agency-wide plans**	**Review 7 years after plan superseded/obsolete.**
ITM/PLA/02	**Final versions of business unit plans**	**Destroy 2 years after plan superseded/obsolete.**
ITM/PLA/03	**Final version of minutes of meetings** Includes minutes and supporting documents tabled at routine meetings held to discuss ITM activities.	**Review 7 years after minutes approved.**
ITM/PLA/04	**Planning process and development of action plans** Working papers documenting the process and development of the plans. Includes drafts, reports, feedback and comments.	**Destroy 2 years after new plan adopted.**
ITM/PLA/05	**Conduct and administration of meetings** Working papers documenting the conduct and administration of meetings. Includes agendas, notices of meetings, draft minutes and supporting documents.	**Destroy 2 years after last action.**
ITM/POL	**POLICY** Records documenting the development and establishment of ITM related policies. Includes proposals and procedures. Excludes Freedom of Information (see ITM/FOI).	
ITM/POL/01	**Information Management Policy** Records documenting the development and establishment of agency's policy related to ITM activities. E.g. ITM security, web, intranet and email, preservation. Includes proposals, reports of consultations and final policy documents.	**Review 5 years after new policy/procedures superseded.**
ITM/POL/02	**ITM-related procedures** Standard agency operating procedures which support established policy. Includes agency manuals, handbooks, directives, etc.	
ITM/RCD	**CONTROL – RECORDS** Systematically controlling all agencies records, regardless of format. Activities associated with creating and maintaining control mechanisms. Includes mail processing. Excludes library catalogues (use ITM/LIB/02).	

ITM/RCD/01	**Mail processing and tracking tools** Documentation for the receipt and despatch of agency mail including classified and registered mail. Includes diaries, registers, copy logs and reports of loss.	**Destroy 5 years after last action.**
ITM/RCD/02	**Documentation for recordkeeping systems** Includes indexes, catalogues and other finding aids.	**Review after system superseded.**
ITM/RCD/03	**Information and records surveys**	**Destroy 5 years after superseded/last action.**
ITM/RES	**RESEARCH AND DEVELOPMENT** Investigations into a subject area associated with the ITM used to support the development of projects, reports, guidance and standards. Excludes: policy and procedures (see ITM/POL) and software development (see ITM/SOF).	
ITM/RES/01	**Research papers** Includes business cases, reports of consultants, major drafts and final documents.	**Review 5 years after reference ceased.**
ITM/SOF	**SOFTWARE DEVELOPMENT** Administering the development of software from conception through to final completion and implementation. Includes **r**equirements, design agreement, usage, maintenance and documentation for software training, use and revisions. Excludes**:** records relating to research, design, implementation and system documentation (refer to Computer Services Department's operational file plan and schedule).	
ITM/SOF/01	**Research** Records documenting the investigation and identification of specific applications to meet business needs. Includes final versions of documentation for all applications, i.e. those that did and did not go into production.	**Review 7 years after software superseded or if software was not implemented, destroy 5 years after last action.**
ITM/SOF/02	**Business requirements** Includes function, behaviour and required performance of software, feasibility studies.	**Destroy 7 years after software superseded or if software was not implemented, destroy 5 years after last action.**
ITM/SOF/03	**Requirement specification/scope document** Copies.	
ITM/SOF/04	**Project plan (signed)** Copy of agreement on system design specifications and copies of revised plans.	
ITM/SOF/05	**Use cases and testing plans** Includes user documentation on cases, procedures and results.	
ITM/SOF/06	**Implementation plans** Includes software training, installation, user manuals, customisation, testing and evaluation.	**Destroy 7 years after plans superseded.**
ITM/SOF/07	**Project plan change history** Requests for changes and copies of CSD initiated changes.	**Destroy 7 years after last action.**
ITM/SOF/08	**Maintenance** Enhancements and corrections.	**Destroy 5 years after last action.**

ITM/SYS	**SYSTEMS ADMINISTRATION** Administering the IT systems and telecommunications appliances at the systems operation level. Records documenting operating systems configuration and installation. Includes monitoring, routine maintenance and up-keep. E.g. back-ups, restores, parts replacement and patches, communications utilities and applications. Also includes documentation for database management, security, routine audits of systems and software and helpdesk.	
ITM/SYS/01	**Software licences**	**Destroy after software is no longer used.**
ITM/SYS/02	**System description manuals** Includes records about what the records and information management systems do and how they work.	**Review once agency is no longer in existence.**
ITM/SYS/03	**System maintenance logs**	**Destroy once information kept on system no longer exists.**
ITM/SYS/04	**Back-up logs**	**Destroy 1 year after last action.**
ITM/SYS/05	**System logs** For history of access or change to data. Includes user access registers, passwords, Internet access logs, audit trails, and documentation for recovery of information on an *ad hoc* basis.	**Destroy 10 years after last action.**
ITM/SYS/06	**Help-desk logs**	**Destroy 1 year after last action.**
ITM/SYS/07	**Maintenance of email systems**	
ITM/SYS/08	**Major breaches of security** E.g. resulting in threat. Either data on computers or hard copies of data.	**Review 7 years after last action.**
ITM/SYS/09	**Minor breaches of security** E.g. resulting in embarrassment.	**Destroy 7 years after last action.**
ITM/SYS/10	**Sanitisation of equipment** Records regarding the permanent removal of all data from digital devices before disposal or reuse.	**Destroy 7 years after disposal of equipment.**
ITM/TEL	**TELECOMMUNICATIONS** Maintaining and updating the agencies Intranet site and/or website to ensure up to date information is displayed. Ensuring that telephones, fax machines, cellular phones, voice mail, local area networks, satellite communication systems and internet connections are well maintained and in good working order. For phone bills, etc. see Financial Management schedule. Includes: voice, video and Internet communications services.	
ITM/TEL/01	**Intranet and Web updates** Includes content audits, versioning and publishing directories.	**Destroy 7 years after final audit or when superseded.**
ITM/TEL/02	**Appliance maintenance logs** Includes records of telephone, switchboard, mobile phones and radio maintenance correspondence. For contracts use FM/ACQ/03.	
ITM/TEL/03	**Telecommunications logs** Usage or assignment of appliance (radio, telephone, fax and computers), e.g. fax machine logs and mobile phone assignment registers.	**Destroy 1 year after last action.**