Ministry of Finance & Planning
Records Management Project

Records Management
Policy & Standards

Prepared by
Allison Consultancy

Status: Issued 1

Report prepared by

JM Wilson
Associate Consultant
Allison Consultancy

Report QA checked by

Mrs J.Y. Allison
Partner
Allison Consultancy

December, 2003

Table of Contents

MOFP Records Management Policy and Standards
Part A - Policy

1. Introduction

The purpose of this policy is to ensure that all staff and other users of records understand what they must do to protect and manage records effectively, efficiently and economically.

This policy is supported by a set of records management standards, which are mandatory across the Ministry of Finance and Planning (hereinafter referred to as 'the Ministry'). These standards will be used to: -

- Measure compliance.
- Identify and promote best practice.
- Support the increased use of electronic records in order to obtain operational benefits without introducing additional risks.
- Comply with the Ministry's information management policy.

This records management policy is based on ISO 15489, the International Standard for records management.

2. Scope

This Policy, together with the associated standards, applies to the management of records, in all technical or physical formats or media, created or received by the Ministry in the conduct of its business activities.

Although not an exhaustive list, examples of items that can constitute records include: -

- Documents (including written and typed documents and annotated copies)
- Computer files (including word processor files, databases, spreadsheets and presentations)
- Electronic mail messages
- Diary records
- Fax messages
- Brochures and reports
- Intranet and Internet Web pages
- Forms
- Audio and video tapes, including CCTV
- Microfiche and microfilm
- Maps and plans
- Photographs
- Printouts from computer systems

3. Applicability

This policy and the associated standards apply to all permanent and temporary employees, contractors, consultants and secondees of the Ministry who have access to records, wherever these records are located.

Policy

Failure to comply with this policy may lead to disciplinary action being taken. It may also leave you liable to prosecution under applicable legislation.

4. Benefits of records management

Adherence to efficient records management practices will enable the Ministry to meet its statutory objectives and overall business responsibilities. Whatever the record media, knowledge and information must be protected, accurate, ordered, complete, useful, up to date and accessible whenever it is needed to:

- Facilitate the business of the Ministry.
- Support implementation of and compliance with the Access to Information Act 2002.
- Ensure compliance with relevant legislation (see section 5 below).
- Facilitate informed decision making at all levels and locations.
- Ensure that the Ministry operates effectively as a prosecuting authority and meets its lawful obligations with regards to the disclosure of evidence.
- Ensure sound governance to satisfy the expectations of the international financial community.
- Ensure that precedents are identified accurately.
- Support continuity and consistency in management and administration
- Protect the rights of employees, regulated entities and the general public.
- Provide an audit trail to meet business, regulatory and legal requirements.
- Promote the activities and achievements of the organisation.
- Support innovative research and development.
- Provide an historical perspective and ensure that relevant material is forwarded to the National Archives.

5. Regulatory environment

The regulatory environment in which the Ministry operates consists of: -

5.1. Statute and case laws, and regulations governing the business environment in which the Ministry operates.

These include, but are not limited to:-

- Access to Information Act 2002
- Financial Audit and Administration Act
- Copyright Act
- Company legislation
- Taxation legislation
- National archives/public records legislation
- Criminal justice legislation
- Civil evidence legislation
- Human rights/civil rights legislation
- Health and safety regulations

5.2. An expectation of the community about what constitutes acceptable behaviour for the Ministry

6. Records Management Policy Statements

Policy

The availability of accurate and relevant information is vital to the efficient management of the Ministry. Our policy is to value records and information as public assets on behalf of all stakeholders. All records will be created and managed efficiently, protected, stored securely and disposed of safely at the appropriate time.

We will comply with all relevant legislation and aim to achieve standards of best practice, including adopted principles deriving from such recognised bodies as the International Organization for Standardization (ISO).

We will ensure that proper records management training, equipment and facilities are provided, and will recruit and train good quality staff (e.g. by establishing a professional development programme).

We will review our records management policy and standards on a regular basis, to ensure applicability and compliance with best practice.

MOFP Records Management Policy and Standards
Part B - Roles and Responsibilities

7. Introduction

The Ministry is the owner of all records created by employees in the course of carrying out Ministry business. Unless ownership is retained by the originator, records received by employees are also owned by the Ministry. Individual employees do not own records but they do have responsibilities for managing records as an integral part of their jobs.

This document describes the roles and responsibilities for managing records within the Ministry.

8. Senior Management Responsibility

The Financial Secretary has overall executive responsibility for the Ministry's records management policy and standards and for supporting the application of the policy and standards throughout the organisation.

9. Records Management Committee

The Records Management Committee is responsible for:

- The approval of any changes to this policy and the associated standards
- The approval of retention and disposal schedules
- The approval of the allocation of protective security markings to record series, files and individual records and any subsequent re-allocation or downgrading of such protective security markings
- The authorisation of the release of registered files and records to the public under the terms of existing and proposed legislation which deals with access to government information.

Additional responsibilities may, from time to time, be given to the Records Management Committee.

10. Documentation and Information Management Services Unit Responsibilities

The Documentation and Information Management Services Unit (hereinafter referred to as Documentation Services) has the following responsibilities.

10.1. Policy and Standards

Documentation Services is responsible for ensuring that the records management policy and standards are kept up-to-date and relevant to the needs and obligations of the organisation, through a process of consultation across the organisation.

Changes to policies and standards will be agreed by the Financial Management Committee.

10.2. Communication and Awareness

Documentation Services is responsible for communicating the records management policy and standards within the Ministry and for ensuring that all staff are aware of their responsibilities for managing records.

10.3. Advice and Guidance

Documentation Services is responsible for providing records management advice and guidance to all staff and other users of Ministry records.

10.4. Training

Documentation Services is responsible for specifying records management training needs and identifying appropriate provision of training for staff across the Ministry.

10.5. Registry Services

Documentation Services is responsible for the provision of registry services to the Ministry. These services include:

- Add list from existing procedures manuals

10.6. Review and Disposition of Records

Documentation Services is responsible for the review and disposition of records. This includes:

- Development and maintenance of retention schedules
- Implementation of retention schedules
- Review of files for which no retention schedules have been defined
- Organising and recording the transfer or destruction of files

10.7. Offsite Storage

Documentation Services is responsible for managing the relationship with the Government Records Centre and any other offsite storage facility.

10.8. 'Orphan' Records

Documentation Services is responsible for obtaining decisions regarding the management of records for which there is no clear Divisional responsibility, for example former Ministry of the Public Service and the Environment records.

10.9. Compliance Monitoring

Documentation Services is responsible for monitoring compliance with the records management policy and standards:

- Within Registries
- Within all Divisions of the Ministry.

11. Line Management Responsibility

11.1. Deputy Financial Secretaries

Deputy Financial Secretaries are responsible for ensuring that these records management policies, standards and procedures are followed across the Division for which they have responsibility. The DFS may nominate representatives within the Division to liaise with Documentation Services.

In certain circumstances (e.g. Financial Investigation Division) responsibility for the Registry may be devolved to a Division. In such cases Ministry records management policies and standards and guidelines **must** be followed.

11.2. Responsibilities of Individuals

Everyone who creates, receives or handles records (as defined above) has a responsibility to follow records management procedures.

12. Monitoring and Auditing

Compliance with records management policy, standards and guidelines may be subject to review and audit by internal and external auditors and other bodies, for example the Jamaican Archives and Records Department (JARD).

MOFP Records Management Policy and Standards
Part C – Standards

13. Determining What Constitutes a Record

Determining which items should be managed as records is based on an analysis of the regulatory environment, business and accountability requirements and the risk of not capturing the records.

Standard – Definition of Records

Business or personal actions should be captured as records and indexed when they:

- **commit an organisation or individual to action;**
- **render an organisation or individual accountable; or**
- **document an action, a decision or decision making process.**

14. Version Control

In some business processes (for example during the development of policy) successive drafts of a document must be retained to provide adequate evidence of the process.

Standard – Version Control

The need to retain successive versions should be determined through the analysis of record keeping requirements and should be documented in procedures.

15. Capture

The purpose of capturing items as records is to: -

- establish a relationship between the record, the creator and the business context that originated it;
- place the record and its relationships within a records system;
- link it to other records; and
- ensure that appropriate audit trails are maintained.

Standard - Capture

Any item that has been identified as a record must be captured by adding it to a registered file.

Until such time as an electronic records management system has been adopted all electronic items that constitute records (including electronic mail, word processed documents and spreadsheets) **must** either:

- be printed and placed on the appropriate registered file; or
- be transferred to CD or other appropriate medium and sent to the registry to be indexed and linked to the appropriate registered file.

16. Registration

The primary purpose of registration is to provide evidence that a record has been created or captured in a records system and an additional benefit is that it facilitates retrieval. It involves recording brief descriptive information or metadata about the record and assigning the record a unique identifier. Registration formalises the capture of the record into the records system.

- a record is registered when it is captured into the records system (this may include the placing of a manual record into a structured filing system or the automated registration of electronic records in an electronic record keeping system); and
- no further processes affecting the record can take place until its registration is complete.

Standard - Registration

Files should be registered by allocating a unique file reference and indexing that file on the Registry File Tracking System.

Individual records should be registered by listing them on a minute sheet which forms part of the registered file.

17. Determining How Long To Retain Records

Decisions about how long records should be retained are based on: -

- an assessment of the statutory and regulatory environment
- business and accountability requirements; and
- the risks associated with retaining or disposing of the record at any particular point in time

Statutory or other regulatory requirements may demand minimum retention periods or submission to an authorising body such as an archival authority or auditors for any necessary approval. The rights and interests of all stakeholders should be considered when determining how long records need to be maintained. The decisions should not be made intentionally to circumvent any rights of access.

Records identified for continuing retention are likely to be those which: -

- provide evidence and information about the organisation's policies and actions,
- provide evidence and information about the organisation's interaction with the client community it 'serves',
- document the rights and obligations of individuals and organisations,
- contribute to the building of the organisation's memory for historical purposes, or
- contain evidence and information about activities of interest to internal and external stakeholders.

Standard – Retention 1

Records should be retained to: -

- **meet current and future business needs;**
- **comply with statutory, legal and corporate governance best practice requirements, by ensuring that the regulatory environment applicable to records management for specific business activities is documented, understood and implemented; and**
- **reasonably meet the current and future needs of internal and external stakeholders.**

Standard – Retention 2

Records that are no longer required should be eliminated as early as possible and in an authorised, systematic manner (see also section 23 below).

Standard – Retention 3

In consultation with the Records Management Committee, Documentation Services should create and maintain retention schedules. Retention schedules should state for how long each record series should be kept together with the justification for the periods specified and the method of disposition.

18. Vital Records

Standard – Vital Records

Vital records must be identified and protected in order to minimise the risk of loss in the event of a disaster. Protection can take the form of secure storage (for example in a fire resistant cabinet) and/or the maintenance of one or more backup copies which are stored in different locations.

19. Subject Classification/Indexing

Subject classification of records, based on business activity acts as a powerful tool to assist the conduct of business and many of the processes involved in the management of records including: -

- providing linkages between individual records which accumulate to provide a continuous record of activity;
- ensuring records are named in a consistent manner over time;
- assisting in the retrieval of all records relating to a particular function or activity;
- determining security protection and appropriate access for sets of records;
- allocating user permissions for access to or action on particular groups of records;
- distributing responsibility for management of particular sets of records;
- distributing records for action; and
- determining appropriate retention periods and disposition actions for records.

19.1. Subject Classification systems

Subject classification systems reflect the business of the organisation, from which they derive and are normally based on an analysis of the organisation's business activities. These systems can be used to support a variety of records management processes.

Standard – Subject Classification

The functions and activities of the Ministry should be reflected in a Corporate File Plan to which records series, files and records can be mapped.

19.2. Indexing

The function of an index is to provide the user with an efficient means of tracing information. An index or indexes should allow the user to: -

- quickly establish the presence or absence of information on a given subject
- identify and locate relevant information within records
- group together information on subjects
- search for information using indexing terms that are appropriate to their needs

Indexing can be done manually or be automatically generated. It may occur at various levels of aggregation within a records system and includes full text indexing.

Standard – Subject Indexing 1

Metadata describing the subject content should be associated with records at the appropriate level of aggregation (i.e. file series, file or record level) in order to meet the anticipated retrieval needs.

Standard – Subject Indexing 2

Record series and registered files should be linked to the Jamaican Government subject indexing scheme that is being coordinated by JARD.

19.3. Vocabulary controls

Subject classification systems and indexes may be supported by vocabulary controls that are suited to the complexity of the records of an organisation. Such vocabulary controls should explain organisation-specific definitions or usage of terms.

19.4. Allocation of numbers and codes

Shorthand methods of referencing records by means other than the title are commonly used. The allocation of numbers or codes is usually undertaken for an aggregation of records. The purpose of coding is associated with a location function, where the number or code indicates the 'address' of the record, which may also be used to retrieve the record.

20. Storage and Handling

Records require storage conditions and handling processes that take into account their specific physical properties. Records of continuing value, irrespective of format, require higher quality storage and handling to preserve them for as long as that value exists.

Standard – Storage and Handling 1

Storage conditions and handling processes should be designed to protect records from:

- **unauthorised access**
- **unauthorised destruction**
- **loss**
- **unauthorised addition**
- **alteration**
- **theft and disaster.**

Standard - Storage and Handling 2

Records should be stored on media that ensure their usability, reliability, authenticity and preservation for as long as they are needed. Issues relating to the maintenance, handling and storage of records arise throughout their existence, not only when they become inactive.

Standard – Storage and Handling 3

Systems for electronic records should be designed so that records will remain accessible, authentic, reliable and useable through any kind of system change, for the entire period of their retention. This may include migration to different software, re-presentation in emulation formats or any other future ways of re-presenting records. Where such processes occur, evidence of these should be kept, along with details of any variation in records design and format.

21. Access and Security

The regulatory environment in which the organisation operates establishes broad principles on access rights, conditions or restrictions that should be incorporated into the operation of records systems. These should take into account legislation covering areas such as privacy, protection of personal information, security, and access to information. Records may contain personal, commercial or operationally sensitive information. In some cases access to the records, or information about them, should not be permitted.

Restrictions on access can be applied both within the organisation and to external users and should protect the legal and other rights of the Ministry, its clients and any other person affected by its actions. Restricted records should be identified only where specifically required by business need or the regulatory environment. Restrictions should be imposed for a stated period, to ensure that the additional monitoring required for these records is not enforced for longer than required. The need to place restrictions on accessibility can change with the passing of time.

Ensuring appropriate access controls is done by assigning access status to both records and individuals.

Managing the access process involves ensuring that: -

- records are categorised according to their access status at a particular time;
- records are only released to those who are authorised to see them;
- encrypted records can be read as and when required and authorised;
- records processes and transactions are only undertaken by those authorised to perform them; and
- parts of the organisation with responsibility for particular business functions specify access permissions to records relating to their area of responsibility.

The monitoring and mapping of user permissions and functional job responsibilities is a continuing process which occurs in all records systems regardless of format.

Standard – Access and Security 1
Formal guidelines should be established to regulate who is permitted access to records and in what circumstances.

Standard – Access and Security 2
It is recommended that the standard set of security markings as described in Section III of the Government of Jamaica Security Handbook be adopted across the Ministry (see also Part E).

22. Tracking

Tracking of the movement and use of records within a records system is required to: -

- identify outstanding action required,
- enable retrieval of a record (to include the ability to track records stored in different media, e.g. electronic and hard copy),

- prevent loss of records,
- monitor usage for systems maintenance and security, and maintain an auditable trail of records transactions (i.e. capture or registration, classification, indexing, storage, access and use, migration and disposition), and
- maintain capacity to identify the operational origins of individual records where systems have been amalgamated or migrated.

22.1. Action tracking

Action tracking may be implemented in a records system for processes where time limits for actions are imposed by or on the organisation. Action tracking:

- allocates steps to be taken in response to decisions or transactions documented in a record;
- assigns responsibility for action to a designated person; and
- records dates by which the predefined action is to be taken and dates when those actions occur.

Action tracking can only be effectively implemented if material is registered into the records system prior to forwarding to the designated persons.

22.2. Location tracking

The movement of records should be documented to ensure that items can always be located when required.

Tracking mechanisms may record the item identifier, the title, the person or unit having possession of the item and the time/date of movement.

Standard – Location Tracking

In order to provide an audit trail, the Registry File Tracking System should track the issue, transfer between persons, and return of registered files to their 'home' registry as well as their disposition or transfer to authorised external organisations including an external store or the Jamaica Archive.

23. Disposition

Retention schedules which govern the removal of records from operational systems should be applied to records on a systematic and routine basis, in the course of normal business activity. No disposition action should take place without the assurance that the record is no longer required, that no work is outstanding and that no litigation, investigation or access request is current or pending which would involve relying on the record as evidence, or supplying it to a requestor.

Disposition action may encompass:-

- immediate physical destruction, including overwriting and deletion;
- retention for a further period within the registry;
- transfer to an appropriate storage area or medium
- transfer to another organisation that has assumed responsibility for the business activity through restructure, sale or privatisation;
- transfer to a storage area managed on behalf of the Ministry by an independent provider where appropriate contractual arrangements have been entered into;
- transfer of responsibility for management to an appropriate authority while physical storage of the record is retained by the creating organisation;
- transfer to an external archive, for example JARD.

Standard – Disposition 1

Records pertaining to pending or actual litigation, investigation or access requests should be clearly identified and should not be destroyed until all outstanding actions have been completed.

Standard – Disposition 2

Disposition should always be authorised by the Records Management Committee. Authority to destroy cannot override the provisions of standard 1.

Standard – Disposition 3

Authorised records destruction should be carried out in a way that preserves the confidentiality of any information they contain and minimises environmental impact.

Standard – Disposition 4

All copies of records that are authorised for destruction, including security copies, preservation copies and backup copies, should be destroyed.

Standard – Disposition 5

A record should be held of which items have been eliminated/destroyed, together with the appropriate authorisations.

24. Characteristics of a record

Records are defined as 'information created, received and maintained as evidence and/or information by an organisation or person, in pursuance of legal obligations or in the transaction of business'.

Standard – Characteristics of a Record 1

A record should correctly reflect what was communicated or decided or what action was taken. It should also be able to support the needs of the business to which it relates and be used for accountability purposes.

Standard – Characteristics of a Record 2

As well as the content, the record should contain, or be linked to, or associated with, the metadata necessary to provide evidence of a transaction, as follows: -

- **The structure of a record, that is, its format[1] and the relationships between the elements comprising the record, should remain intact.**
- **The business context in which the record was created received and used should be apparent in the record (including the business process of which the transaction is part, the date and time of the transaction and the participants in the transaction, i.e. an audit trail of the transaction).**
- **The links between items held separately but combining to make up a record should be present.**

[1] In this context, 'format' refers to the layout of the record, not the medium in which it is stored nor the PC file type.

Standard – Characteristics of a Record 3

Records management procedures and practices should result in authoritative records which exhibit the characteristics of authenticity, reliability, integrity and usability.

Standard – Characteristics of a Record 4

Items which do not constitute records (for example personal electronic mail messages) should not be placed in record keeping systems and should be disposed of as soon as possible *(and in any case within 30 days).*

24.1. Authenticity

An authentic record is one that can be proven: -

- to be what it purports to be;
- to have been created or sent by the person purported to have created or sent it;
- to have been created or sent at the time purported, and
- to be credible and authoritative so that evidence can be safely derived from it (for example to be used in courts etc.)

Standard – Authenticity

To ensure the authenticity of records the Ministry should implement and document procedures which control the creation, receipt, transmission, maintenance and disposition of records to ensure that record creators are authorised and identified and that records are protected against unauthorised addition, deletion, alteration, use and concealment.

24.2. Reliability

A reliable record is one whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.

Standard – Reliability

Records should be created at the time of the transaction or incident to which they relate, or soon afterwards, by individuals who have direct knowledge of the facts or by instruments routinely used within the business to conduct the transaction.

24.3. Integrity

The integrity of a record refers to its being complete and unaltered.

Standard – Integrity

Records should be protected against unauthorised alteration. Divisional records management procedures should specify what additions or annotations may be made to a record after it is created, under what circumstances additions, or annotations may be authorised, and who is authorised to make them. Any authorised annotation to a record should be explicitly indicated and traceable.

Any addition or deletion to a record should constitute the creation of a new record, and be captures into the system as such.

24.4. Usability

A useable record is one that can be located, retrieved, presented and interpreted. It should be capable of subsequent presentation as directly connected to the business activity or transaction that produced it. The contextual linkages of records should carry the information needed for an understanding of the transactions that created and used them. It should be possible to identify a record within the context of broader business activities and functions. The links between records that document a sequence of activities should be maintained.

Standard – Usability

Records should be arranged in an authorised record keeping system that enables the Ministry to obtain maximum benefit from quick and easy retrieval of information.

MOFP Records Management Policy and Standards
Part D - References and Links

British Standards Institution (BSI). *Information and documentation – guidelines for the content, organization and presentation of indexes*. BS ISO 999:1996

British Standards Institution (BSI). *Information security management.* BS 7799 parts 1 and 2:1999

British Standards Institution (BSI). *Recommendations for examining documents, determining their subjects and selecting indexing terms*. BS 6529:1984

Government of Jamaica. *Security Handbook* [full reference to be added by MoF&P as only a partial photocopy was provided to Allison Consultancy – it was not possible to determine the date of this document or the full title]

Hare, C.E. and McLeod J. *Developing a records management programme.* Aslib, London, 1997.

International Organization for Standardization (ISO). *Information and Documentation – Records management*. ISO/DIS 15489 2000

International Organization for Standardization (ISO). *Information and Documentation – Documentation storage requirements for archive and library materials*. ISO/IEC DIS 11799

Robek, M.F., Brown, G.F & Maedke, W.O. *Information and Records Management.* 3rd ed. Glencoe, 1987.

MOFP Records Management Policy and Standards
Part E – Security Markings

Extract from Section III of the Government of Jamaica Security Handbook

An official document must be protected if harm would result from the disclosure of the information it contains to an unauthorised person. The degree of protection required will vary. The following four security classifications indicate what precautions must be taken when handling a particular document:

TOP SECRET

SECRET

CONFIDENTIAL

RESTRICTED

These security markings are defined in the following table. Guidelines for handling documents that carry a security marking form part of the Records Centre Manual.

Protective Marking	International Relations	Defence	Security & Intelligence	Public Order & Private Rights	Economic Interests	Law Enforcement	Policy and Operations of Public Service
TOP SECRET	Cause exceptionally grave damage to relations with friendly governments. Threaten directly the internal stability of friendly countries.	Cause exceptionally grave damage to the effectiveness or security of Jamaican or allied forces.	Cause exceptionally grave damage to the continuing effectiveness of extremely valuable security or intelligence operations.	Lead directly to widespread loss of life. Threaten directly the internal stability of Jamaica.	Cause severe long-term damage to the Jamaican economy.		
SECRET	Raise international tension. Damage seriously relations with friendly governments.	Cause serious damage to the operational effectiveness or security of Jamaican or allied forces.	Cause serious damage to the operational continuing effectiveness of highly valuable security or intelligence operations.	Threaten life directly. Seriously prejudice public order, or individual security or liberty.	Cause substantial material damage to national economic and commercial interests.		
CONFIDENTIAL	Materially to damage diplomatic relations (i.e. cause formal protect or other sanction).	Cause damage to the operational effectiveness or security or intelligence forces.	Cause damage to the effectiveness of valuable security of intelligence operations.	Prejudice individual security or liberty.	Work substantially against national economic and commercial interests. Undermine substantially the financial viability of major organisations.	Impede investigation of serious crime. Facilitate the commission of serious crime.	Impede seriously the development or operation of major government policies. Shut down or otherwise substantially disrupt significant national operations.
RESTRICTED	Affect adversely diplomatic relations.	Make it more difficult to maintain the operational effectiveness or security of Jamaican and allied forces.		Cause substantial distress to individuals. Breach proper undertakings to maintain the confidence of information provided by third parties.	Case financial loss or loss of earning potential to or facilitate improper gain or advantage for individuals or companies.	Prejudice the investigation of crime. Facilitate the commission of crime.	Impede the effective development or operation of government policies. Breach statutory restrictions on disclosure of information. Disadvantage government in commercial or policy negotiations with others. Undermine the proper management of the public sector and its operations.