CAYMAN ISLANDS
NATIONAL ARCHIVE
PORTFOLIO OF THE CIVIL SERVICE
CAYMAN ISLANDS GOVERNMENT

RECORDS AND INFORMATION MANAGEMENT STANDARD

S2

MAY 2017

ISSUED UNDER THE NATIONAL ARCHIVE AND PUBLIC RECORDS LAW (2015 REVISION), SECTION 7

Deputy Governor's Foreword

Sound management of public records and information is the cornerstone of good governance. It promotes accountability and transparency, and having a robust information management strategy in place ensures better information for a more efficient government.

To ensure that the Cayman Islands Public Service is at the forefront of modern and innovative approaches to information management, we need to find ways to continuously improve how we think about our information needs, both now and in the future. This can be achieved by giving careful consideration to the modernised and evolving context in which we operate, and the tasks required to stay at the forefront of technological advancements that can enhance service delivery.

To attain our aspirational goals of becoming a World Class Civil Service, we need to continue to evaluate our operating context, improve our services and strive to move beyond the boundaries of what is attainable. This will allow departments, Ministries, Portfolios, Civil Servants and the people of the Cayman Islands to gain the most value from our information assets.

Therefore, the purpose of the Records and Information Management Standard is to provide guidance to public agencies to assist with compliance measures set out in the *National Archive and Public Records Law (2015 Revision).* Adherence to the principles set out in this Standard promotes the Government's vision to become open and accountable to the people of the Cayman Islands. This goal, facilitated through the Cayman Islands National Archive, is to ensure that a high standard of records and information management practices are adopted across the entire public service.

I trust that this Standard will not only upgrade records and information management throughout the public service, but that it will enable Portfolios, Ministries and their agencies to be more effective and efficient in serving the public.

_____

Hon. Franz Manderson, JP
Deputy Governor

Table of Contents

1. Introduction

The business of the public service is fundamentally information based, and as such a high value should be placed on how that information is managed, accessed, shared, protected, re-used, and disposed when no longer required for business needs. Most public service agencies' information is widely dispersed, stored on computer hard drives, shared network drives, and legacy paper files, with key tacit knowledge of the public service captured in the minds of our Public Servants. These information assets together form the corporate memory of the Cayman Islands Public Service.

This Standard is created as a practical tool to support public agencies in meeting their obligations under the *National Archive and Public Records Law (2015 Revision)*. It will assist the wider goals of government by ensuring a transparent, accountable, consistent and robust approach is applied across the public service, within the evolving and modernised government landscape.

Implementing an information management strategy requires that the public service adopts a sound records and information management infrastructure. This can only be achieved if agencies work collaboratively to create and manage these assets, which support current and future business needs, decisions and obligations.

1.1 Benefits of Active Records and Information Management

The public service should continually investigate ways to improve the way government information assets are managed by strategically examining the type of information we create and how we manage it. The actualised benefits from this process can be experienced at many levels - the individual and departmental levels, within the wider public service, and especially by our customers (members of the public) we serve.

Potential benefits include:-

- Compliance with relevant legislation.
- A foundation for sustainable and effective service delivery that allows public agencies to optimise the use of information to improve their service delivery standards.
- Efficiency in our decision making and policy development, for example, agencies being able to locate information when required, thereby minimising the need to re-invent the wheel.
- Corporate knowledge of the agency is known by staff (where it is stored, how it is saved, protected and eventually disposed of when no longer required for business transactions).

- Ongoing public decisions of national significance are captured and held for perpetuity, documenting our history.
- A reduction in information related risks.
- A platform for participatory and collaborative ventures by making the best use of information, as well as sharing and re-using information.
- Increased transparency in the information held by public agencies, enabling the public to hold government to account.
- Greater understanding of what each agency does, thereby allowing for higher levels of public engagement with government as a whole.

1.2 The Need for a Records and Information Management Standard

There is a clear need for accountability, with each public servant taking responsibility to ensure that the same duty of care is applied to information, as with other government assets. All public service agencies should be confident that they have a holistic understanding of their information needs, both now and for the changing public sector landscape ahead. This will require effective planning to warrant that agencies are in a state of readiness as a means of addressing areas such as risk management, short-term requirements, accessibility, long-term preservation, and ongoing staff development.

The Cayman Islands National Archive is committed to assisting public agencies with the implementation of records and information management best practices, so that value from these corporate assets are realised and properly managed in accordance with relevant guidance and legislation.

Seeking to meet the criteria set out in this Standard will help public entities to take a more integrated approach to managing their information needs. It should be read in tandem with other published standards, policies or guidance issued by the Cayman Islands National Archive under the *National Archive and Public Records Law (2015 Revision).*

1.3 Mandate

Section 7 of the above Law states that the Cayman Islands National Archive, "*may, with the approval of the Deputy Governor, draw up and issue standards relating to all aspects of records management by public agencies*."

Public agencies, as defined by the National Archive and Public Records Law, must be committed to establishing and maintaining information management practices that meet accountability/compliance requirements, business needs and stakeholder expectations. As assets, information and records must be trustworthy, properly described, well managed, protected and readily accessible throughout their life cycle. Additionally, in

accordance with the Law, public agencies shall, *"create, manage and dispose of its public records in accordance with any prescribed standard*", thereby providing for full and accurate records which are:-

- **compliant** with the record keeping requirements established by the National Archive, or by other regulatory bodies and laws;
- **fit for purpose** to meet current business needs;
- **created in a format** that can enable efficient business processes and maximise its potential for use;
- **adequate** for the purposes for which they are kept;
- **complete** in content and containing the structural and contextual information necessary to document a transaction;
- **meaningful** with regards to information and/or linkages that ensure the business context in which the record was created and used is apparent;
- **comprehensive** in documenting the complete range of business for which evidence is required by the organisation;
- **accurate** in reflecting the transactions they document;
- **authentic** in providing proof they are what they profess to be and their author(s) did indeed create them; and
- **inviolate** through being securely maintained to prevent unauthorised access, alteration or removal.

2. Purpose

The purpose of this Standard is to provide a governance framework for public agencies to establish internal practices for the creation, management and control of their records and information, in addition to outlining staff responsibilities.

3. Policy Statement

The Cayman Islands Public Service is committed to establishing and maintaining information management practices that meet its accountability requirements, business needs and stakeholder expectations. Compliance with the Records and Information Management Standard will ensure information created by agencies is trustworthy, properly described, well managed and accessible to all staff when required.

4. Scope

This Standard applies to all public agencies and their staff, and covers all records and information created, managed and received to support each agency's business activities,

regardless of format, medium or age; as well as all business applications used to create corporate information.

Out of scope of this Standard are the records and information held by the Governor of the Cayman Islands, which belong to the Government of the United Kingdom of Great Britain and Northern Ireland (whether they are created or held in the Cayman Islands or elsewhere). In addition, this Standard does not cover collections of published reference materials, historical archives or artefacts such as those found in archives or museums.

The goals of this Records and Information Management Standard are to:-

- Retain important records and information for reference and future use.
- Dispose of records and information, in accordance with the relevant approved disposal schedule, when they are no longer required for business needs.
- Manage important information for efficient retrieval and ease of access.
- Ensure that all public servants know what information should be retained, how long it should be kept, how long it should be stored, and when and how it should be destroyed.

Public records and information that is poorly managed can:-

- Undermine the rights of government and its citizens.
- Have an adverse effect on decision making, leading to a negative reputation for public agencies or government in its entirety.
- Lead to an increase in costs, inefficiencies and liabilities due to the disposal of essential records and information or the retention of unnecessary information.

5. Strategic Context

Public agencies are in a state of transition, moving from a paper record environment towards modern digital platforms, however there has been no overarching approach to this transition. As global trends moved towards a more electronic environment, the Cayman Islands Government information management practices were still lagging behind, and in some instances the impact has been a loss of control of information, to not being able to access information in a timely manner. For example, poor records and information management practices has been cited in recent reports from the Office of the Auditor General and the Information Commissioner as a contributory factor in agencies not being able to respond to inquiries or provide supporting information when required. In efforts to modernise its approach to the delivery of public services, some entities have made a conscious effort to be at the forefront of technological advancements, and implemented

the concept of the 'paperless office'. However, moving solely to an electronic or paperless environment has proved difficult, given financial and practical constraints.

In efforts to meet the aspirational goal of being a World Class Civil Service, public entities are looking towards the provision of e-services, and other electronic platforms to provide services that are customer centric and represent value for money. Therefore, the need for an information management strategy that governs how we manage and protect records becomes more crucial.

All public agencies should strive for a holistic approach towards the management of their corporate information, and seek to integrate its procedures within the broader information management strategies of Government. This includes implementation of the following:

- *Creation, Maintenance and Disposal Records Management Standard S1*
- *The Deputy Governor's Code of Practice on Records Management*
- Approved Administrative File Plans and Disposal Schedules -
    - *Financial Management*
    - *Human Resource Management*
    - *Buildings, Equipment and Vehicle Management*
    - *Communications Management*
    - *Information and Technology Management*
    - *Strategic Management*
    - *Transitory Records*
- *Government Electronic Resources Policy.*

6. Regulatory Framework

Each public agency should recognise its statutory obligations and be accountable for its actions, ensuring compliance with relevant legislation which includes:

- *The Cayman Islands Constitutional Order 2009*
- *National Archive and Public Records Law (2015 Revision)*
- *Freedom of Information Law (2015 Revision)*
- *Evidence Law (2011 Revision)*
- *Electronic Transactions Law (2003 revision)*
- *Public Management and Finance Law (2013 Revision) and Regulations (2013 Revision)*
- *Public Service Management Law (2013 Revision) and Personnel Regulations (2013 Revision)*
- *The Copyright (Cayman Islands) Order 2015*
- *Data Protection Law (2017).*

7. Electronic Records and Information Management Systems

7.1 Electronic records are created and stored in a variety of ways in the Cayman Islands Public Sector. They can be born digitally, i.e. created electronically via computer software, or scanned from pre-existing hardcopies. These records include word-processed documents, spreadsheets, emails, images, videos and audio. Records can be found in agency-specific business applications systems (such as the Geographical Information System for the Lands and Survey Department), shared (network) folders, hard drives and removable media. Electronic records and information can be efficiently created, stored, accessed and disposed (when no longer needed), but ensuring that the appropriate format, security and user restrictions are enabled and managed as long as the records and information are required for business needs.

7.2 Public agencies should aim to develop an infrastructure to support electronic records management, and work towards implementing an Electronic Records Management System (ERMS), or other systems such as an Electronic Document Management System (EDMS) or Electronic Content Management System (ECM). These systems should prevent the unauthorised access, duplication, alteration, removal, or destruction of records and information, and ensure the information is accessible and retrievable for as long as required, as this provides audit trails of all actions undertaken. Electronic records should only be printed when necessary for legal or business continuity purposes.

When procuring the above systems, agencies must make sure they are compatible with Government's technological infrastructure and that they incorporate the following processes:

- creation and capture of records;
- control, access and tracking of records;
- protection of record integrity, reliability and authenticity;
- security (including data classification) and storage of records;
- disposal of records in accordance with approved disposal schedules; and identification of vital records.

7.3 Storing large volumes of unstructured data may pose a potential operational risk when trying to retrieve and manage information. Whereas, utilisation of the above systems provide governance and central control, and allow searches across corporate information through keywords, and so forth. For more guidance, agencies should contact Computer Services Department or your ICT provider.

7.4 The preservation of electronic records ensures that the information is accessible and useable. Public agencies' Continuity of Operations Plans (CoOP) should include protection and recovery strategies which help to reduce environmental factors (e.g. water/fire damage and recovery), the migration of the data to keep up-to-date with technology (software and hardware), and the implementation of routine backups.

7.5 Shared drives can be used as a temporary measure in absence of a records and information management system. However, when using shared drives, appropriate access controls and protocols should be in place to prevent unauthorised access. This will contribute to the authenticity of records managed therein. Additionally, folders can be created to mirror the agency's file plan to provide for ease of access in locating records, which supports information-sharing across the agency by providing a group workspace.

7.6 Public agencies must ensure that the necessary metadata is captured and managed properly along with the associated records and information to which it relates. Metadata provides consistent identification of records, preserving their authenticity, and implementing retention and disposition requirements. The necessary metadata elements should be clear and concise, describing why, how and by whom the information was created or digitised, including details about their structure and content, history and use. e.g. when it was digitised/captured in the information management system, and when and who accessed/changed it. This will facilitate in describing and organising electronic content to allow users to find, manage, control, understand and preserve records and information over time. Essential elements to capture include title, date, author(s), as well as structural and administrative information, e.g. format, file name/path, storage location/URL, subject, access information and keywords. Associated metadata is automatically created when using shared drives in a Windows operating system. This data is found in the 'Properties' functionality and provides details such as when it was created, date and time it was last saved, author and size.

7.7 All records need to be uniquely identifiable. Version control helps to preserve the authenticity of a record and it will also assist in providing an audit trail for future tracking of record development. The principle of naming conventions is to use set rules that are applied to label all records and electronic folders, ensuring consistency, and facilitating easier access. Names for records must be meaningful, succinct, and convey the subject of the content. Version control and naming conventions should be documented within the agency so that all staff are familiar with and know how to use them. For further information, agencies should consult related National Archive guidance.

7.8 Records and information may be stored in systems outside the agency's ownership and control. Core government business applications such as IRIS and TRS hold essential information for many agencies, but are managed centrally.

7.9 For information management processes to be seen as a seamless day-to-day activity, it is important that they are designed in consideration of workflows and users, ensuring successful integration with the agency's business operations.

8. Capture, Control and Maintenance of Information

8.1 Under Section 6(1), the National Archive and Public Records Law (2015 Revision), all public agencies have an obligation to create "full and accurate public records of its business and affairs". Thus, an agency's records and information system should be dedicated to creating, capturing and maintaining authentic, reliable and useable records which meet the needs of internal and external stakeholders. Information assets must be maintained for as long as they are required to effectively and efficiently support the business functions and activities of that agency. For long-term retention and digital continuity, agencies will need to consider appropriate formats, such as PDF/A and JPEG2000.

8.2 All information created or received by an agency should be captured into the records and information management system unless classified as a transitory record; this includes unofficial emails, duplicates, background research, etc. Transitory records need only be retained for a short term so as to enable the completion of a routine action or final record. Despite their temporary nature, these records must be kept accessible and stored securely until the retention has expired, as noted in the *Disposal Authorisation for Transitory Records: Administrative Schedule No. 8*.

8.3 Emails which are created and received during the course of government business provide evidence of official transactions and decisions, and should be administered accordingly. Emails, as public records, can be subject to Freedom of Information requests, and therefore need to be managed effectively with appropriate measures, which may include:-

- Using folders to organise messages – establish a structured file directory by using subject or activity.
- Disposing of email which has short-term value and is covered by the approved administrative Transitory Schedule.
- Downloading or storing official emails/attachments – storing emails that document business transactions should not be stored in email inboxes, but should be placed in

relevant places, for example, shared folders or electronic content management systems, for accessibility and long-term management and storage.

- Limiting the use of attachments for email/information exchange – utilise more secured methods to share information, such as Dropbox. Contact the Computer Services Department for more guidance.
- Using distribution lists and groups – minimise the use of misdirected emails by ensuring that appropriate groups or lists are set up as part of your collaborative framework.

8.4 It is essential that all public servants store official information and records on the entity's recordkeeping system. Public records should not be maintained in email inboxes, U drives, PC or laptop hard drives, or on removable/external media (e.g. CDs, USB drives). These electronic storage facilities do not contain records and information functionality, and the Computer Services Department does not back up local hard drives or external media. Furthermore, they can be subject to an array of technological issues, thereby increasing the risk of losing records, which may not be recoverable. Additionally, they cannot ensure records will be managed and maintained over time, in order to support and provide evidence of business activities. It is recommended that these storage formats be used for reference copies only.

9. Information Security

9.1 Good information management underpins good information security. All staff should have access to information for ongoing operational use, unless the information requires a specific security restriction. When handling public records, staff should be reminded of their obligations under the *Public Service Code of Conduct*, the Freedom of Information Law and/or conditions identified in their employment contract. All employees should exercise good judgment, take responsibility and be accountable for the information they handle on behalf of their agency.

9.2 Access restrictions should not be imposed unnecessarily, but used to protect:

- individual employees, or client privacy and personal information.
- sensitive material, such as security classified material.

9.3 All information has a value according to its sensitivity and this is occasionally illustrated through security/data classifications associated with the records, e.g. *Confidential*, *Restricted*, etc.

9.4 Cyber security is an important aspect to consider and it is an area which the Cayman Islands Government is committed to building resilience. Mechanisms are currently in place to be proactive, rather than reactive, in analysing threats, vulnerabilities, and potential impacts associated with daily business activities. For more information and advice on cyber security, contact the e-Government unit in the Cabinet Office or the Computer Services Department.

9.5 Public agencies may choose to layer their security, including the use of perimeter controls, security alarms and access panels, or to ensure that the rented facility or other off-site storage locations where records and information are stored have appropriate access and security controls.

9.6 Agencies should ensure that necessary measures are in place for the protection of records and information, which includes the identification of vital records as part of their Continuity of Operations Plan. Plans should incorporate mitigating measures to safeguard their information assets from threats such as a hurricane or other disasters.

10. Release of Publicly Available Information

10.1 In accordance with obligations under Freedom of Information legislation, and in the spirit of open-government policies, access to publicly available information should be provided on the agency website as part of their Publication Scheme.

10.2 The general public, both locally and abroad, have a right to apply for access to information held by the agency under the *Freedom of Information Law (2015 Revision).* This applies to all information held by the agency, whether in corporate information management systems or in personal stores such as email folders or shared and personal drives. Responses to applications for access under FOI are the responsibility of the Information Manager or Deputy Information Manager of each public authority. For more information please consult the related legislation or your agency's Information Manager.

11. Disposal of Records and Information

11.1 All records, regardless of format or location, are to be retained and disposed of in accordance with disposal schedules issued by the National Archive and approved by Cabinet. Employees of each public agency must be made aware of these policies/guidance, and understand the importance of timely destruction in addition to the corresponding penalties of unauthorised destruction. The disposition of records and information must be documented and retained by the public agency to provide evidence

that the records were disposed in accordance with prescribed methods. For more information on records and information disposal contact the National Archive for assistance.

11.2 Public agencies should actively apply both administrative and operational schedules which will help to reduce the cost of storage, and ease in transitioning to a digital environment. Agency records and information may be destroyed when they reach the end of their required minimum retention periods, as set out in Cabinet-approved disposal schedules. The retention takes into account all business, legal and government requirements for the information. Records and information should not be destroyed (even if the retention has expired), if –

- there are outstanding operational or legal obligations to retain them;
- records are subject to outstanding Freedom of Information requests;
- records are subject to an outstanding audit, or on-going investigation or court case; or
- records are under review by the Cayman Islands National Archive.

11.3 When deleting electronic records, public agencies should ensure that the records are permanently deleted from the agency's IT infrastructure. The use of the delete function in software packages may not be sufficient to destroy electronic records. Public agencies may need to contact the Computer Services Department or their individual IT provider for further guidance on appropriate procedures. If duplicate records and information are involved, both copies must be destroyed or deleted where appropriate, and in accordance with an approved disposal schedule. Failure to destroy duplicates, when the original has been destroyed, is a risk and may open the agency up to liability. For example, in the case of an FOI request, if the relevant records were destroyed, but the duplicates exist, they must be produced/used to address the FOI inquiry.

11.4 The disposal of transitory records is governed by the *Disposal Authorisation for Transitory Records: Administrative Schedule No. 8*. Prior to destruction, temporary records and information should be reviewed to ensure they are no longer required for business need, drafts have been finalised, and final records captured in the official recordkeeping system. Additionally, records and information should not be destroyed if they are subject to an FOI request, or needed for legal or financial purposes (e.g. audits).

11.5 Each agency shall enter into arrangements with the National Archive for the transfer of records and information identified as archival, which have reached the end of its retention and are no longer required for the agency's business purposes, but may have historical value.

11.6 All required records, regardless of format, shall also be transferred to relevant agencies as a result of an agency restructure or administrative change, e.g. reassignment of functions following an election. Contact the National Archive for further guidance on the movement of records.

12. Roles and Responsibilities

The National Archive and Public Records Law, section 6(2)(a) and (b) states that it is the responsibility of the "*most senior officer in every public agency to ensure that public records of that public agency…are maintained in good order and condition…created, managed, disposed of in accordance with records management standards and disposal schedules drawn up under this Law*." However, all staff have responsibilities in managing agency's records and information, as noted below:

Roles	Responsibilities
Chief Officers or Head of Departments	• Implement the *Records and Information Management Standard* and ensure compliance with all relevant statutory and regulatory requirements. • Manage informational assets across the organisation – by providing timely, appropriate, accurate, and up-to-date information at the point of need, e.g. for an FOI request. • Assess and manage risks on the confidentiality, quality, integrity, and availability of information. • Be accountable for the overall records and information management practices of the agency, including the creation and control of records, development of an operational disposal schedule, and protection of information assets from damage and unauthorised access/alteration or destruction. • Provide sufficient support and resources for ensuring a sustainable records and information management programme is integrated into business processes, systems and services. • Uphold compliance with the relevant legislation and the National Archive's recordkeeping standards and guidance. • Ensure information is of the appropriate quality, and in the relevant media, to support organisational needs. • Support and foster a culture amongst their staff to

	enable compliance with and promote good information management practices. • Disseminate information management policies, procedures, tools and systems to all staff. • Ensure staff are appropriately educated, trained, and understand and comply with the Records and Information Management Standard, including the knowledge and implementation of other records and information management guidance and policies issued by the National Archive
Managers and Supervisors	• Assume ownership and responsibility for the management of information created and used within their areas of operation. • Ensure the information is accurate, fit for purpose and has appropriate access and security permissions assigned. • Monitor staff under their supervision to ensure that they understand and comply with information management policies and procedures.
Information Managers	• Ensure that information management practices comply with legal obligations. • Develop, maintain and review records and information management policies, procedures, tools and systems. • Develop and annually update the Publication Scheme. This includes the proactive publication of open records and information. • Provide public access to information under the *Freedom of Information Law*. This includes liaising with applicants on the receipt, analysis and assessment of FOI requests. • Liaise with the Freedom of Information Unit. This includes compiling and reporting all required statistics. • Receive complaints and prepare for appeals before the Information Commissioner. • Liaise with Computer Services Department and private vendors to maintain the technology used for managing electronic records. • Network with other Information Managers to share knowledge and solve common issues. • Deliver or arrange information management training for agency staff.

	• Monitor staff compliance and report to the Chief Officer or Head of Department. • Any other responsibilities specific to your agency.
IT Managers, if applicable, or inquire with Computer Services Department or other service provider	• Ensure IT platforms are fit for purpose with the essential functionality to meet business and record and information management needs • Assume responsibility for the day-to-day maintenance of electronic systems that store records. • Work in conjunction with the records/Information Manager to ensure that public records are properly managed, protected and appropriately preserved for as long as they are required for business, legal and long-term preservation purposes. • Ensure that all electronic systems capture appropriate system-generated metadata and audit trail data for all electronic records to ensure that authentic and reliable records are created. • Ensure that electronic records in all electronic systems remain accessible by migrating them to new hardware and software platforms on a regular basis, and when there is a danger of technology (media and format) obsolescence. • Ensure that all data, metadata, audit trail data, operating systems and application software are backed up on a daily, weekly and monthly basis to enable the recovery of authentic, reliable and accessible records should a disaster occur. • Ensure that backups are stored in a secured manner until no longer needed, and then disposed of (deleted or transferred to the National Archive's Historical Collections) in accordance with approved disposal schedules.
Records Officers	• Apply recordkeeping rules as directed by the Information Manager. • Use approved file plans to classify and name records. • Create, capture and close records in accordance with the approved disposal schedules. • Use information management tools to search for records in response to FOI requests, under the supervision of the Information Manager. • Arrange retrieval of records to/from storage

	locations. • Report to the Information Manager on FOI and records management activities. • Apply disposal schedules (operational and administrative) to transfer or destroy records, and arrange and document disposal. • Periodically follow up with the National Archive to ensure proper retention periods are in place. • Support and advise other staff in the use of electronic records management systems, and the file plan and disposal schedule for the creation, filing, classification, retention and disposal of records.
All agency staff	• Treat information as a corporate asset. • Take ownership for the information they create, capture or maintain. • Take ownership for their role in the effective management of the information created and used in their organisational unit. • Make information accessible to those who require it to fulfil their duties. • Ensure that they are always aware of and respect the confidentiality of information they produce, share or receive. • Understand the recordkeeping obligations and duties that relate to their position. • Only destroy records under a Cabinet approved disposal schedule (administrative and operational for agency specific records).

13. Monitoring

13.1 Staff and system compliance with this Standard should be monitored within each public agency and the outcomes regularly reported to senior management.

13.2 Under section 9 of the *National Archive and Public Records Law (2015 Revision*), the National Archive "*shall monitor the management of public records by public agencies and may from time to time conduct such inspections of the public records and records management practices of public agencies*". In accordance to Section 10, if any "*records management practices of a public agency are inadequate*", the National Archive will advise the Deputy Governor and the Chief Officer of the relevant agency.

13.3 Staff and system compliance with this Standard will be monitored by the National Archive, with outcomes reported at least annually to the Deputy Governor.

14. Noncompliance

14.1 Failure to maintain records in accordance with National Archive standards and guidance could subject public agencies to penalties and fines as detailed in section 11 of the National Archive Law –

"(1) A person who, knowing that he does not have proper authority under this Law to do so, intentionally -

(a) damages or alters a public record of a public agency; or

(b) disposes of such a public record or removes any public record from official custody, commits an offence and is liable on summary conviction to a fine of two thousand dollars or to imprisonment for a term of six months, or to both.

(2) Where a person's neglect of official duties results in damage to or the destruction of a public record, that neglect shall be grounds for discipline or dismissal of that person."

14.2 Non-compliance should be reported to the head of the agency as soon as possible. If the non-compliance involves the head of the agency or Chief Officer, a report should be made to the Deputy Governor at deputy.governor@gov.ky.

15. Review

This Standard will be reviewed annually, or earlier if required by changes in business or the regulatory environment to consider its relevance, continuing appropriateness and staff awareness of its requirements.

16. Authorisation

This Standard has been approved by:

Name:	Franz I. Manderson
Position title:	Deputy Governor
Agency Name:	Deputy Governor's Office in consultation with the National Archive
Signature:	
Date:	

17. Definitions

Business Applications - any software or set of computer programs used by business users to perform various business functions.

Electronic Record - A record that is processed and maintained by electronic means, that has both content and metadata. This includes any combination of text, data, graphics, sound, moving pictures or any other forms of information.

Digital Continuity - the ability to use digital information in the way that you need, for as long as you need.

Digital Repositories - a mechanism for managing and storing digital content.

Information - produced through processing, manipulating and organising data to answer questions. Includes data, text, images, sounds, codes, computer programmes, software and databases.

Information Assets - a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently.

Metadata - structured information that describes and/or allows users to find, manage, control, understand or preserve other information over time.

Public Agency, as defined under the *National Archive and Public Records Law (2015 Revision)*, section 2, includes-

(a) the Cabinet;
(b) the Legislative Assembly;
(c) a ministry, portfolio or department;
(d) a statutory body or authority, whether incorporated or not;
(e) an office established by any Law;
(f) a court or tribunal;
(g) a company in which the Government has a controlling interest, or any subsidiary of such a company; or
(h) a prescribed person or body.

Public Record - information, in any form, created, received, or maintained by a public agency in the course of, or as evidence of, a transaction or activity effected or undertaken in the conduct of its business or affairs; (*National Archive and Public Records Law* s2.)

Transitory Records - records, in any format, generated or received by an entity during the course of normal business operations, which have limited value once usefulness has ceased for the completion of a routine task, or in preparation of a final record.

Vital Records - Records identified as essential for the continuing conduct of an organisation's business, including the re-creation of its legal status and determining the rights and obligations of its stakeholders.

Standard Information

File Reference	GRM/STA/04
Policy Name:	*Records and Information Management Standard S2*
Related legislation/applicable section of legislation:	• *National Archive and Public Records Law (2015 Revision)* • *Freedom of Information Law (2015 Revision)* • *Evidence Law (2011 Revision)* • *Electronic Transactions Law (2003 revision) (Under Review)* • *Public Management and Finance Law (2013 Revision) and Regulations (2013 Revision)* • *Public Service Management Law (2013 Revision) and Personnel Regulations (2013 Revision)* • *The Copyright (Cayman Islands) Order 2015* • *Data Protection Legislation [upcoming]*

Related policies, procedures, guidelines and standards:	• All Cabinet approved Administrative and Operational Disposal Schedules –
	  ○ *Financial Management*
	  ○ *Human Resource Management*
	  ○ *Buildings, Equipment and Vehicle Management*
	  ○ *Communications Management*
	  ○ *Information and Technology Management*
	  ○ *Strategic Management*
	  ○ *Transitory Records*
	• *Creation, Maintenance and Disposal Records Management Standard, 2010.* Cayman Islands National Archive Records Management Standard S1
	• *Guideline 1- Destruction of Public Records*
	• *Guideline 3 - Implementing the Government Use of E-mail Policy*
	• *Guideline 8 - Managing Electronic Records*
	• *Fact Sheet 1 - CINA Legal Admissibility of Electronic Records*
	• *Fact Sheet 5 - Cloud Guidance and Checklist*
	• *Fact Sheet 6 - Transitory Records*
	• *Administrative Circular No. 2 of 2006 – Government Use of Email*

Approved by:	Franz I. Manderson, Deputy Governor
Approval date:	
Effective date	
Review date	*April 2018*
Version	*V1.0*

Consideration was given to the following in the development of the Standard:

- *National Archive and Public Records Law (2015 Revision).*
- *Freedom of Information Law (2015 Revision).*
- *Creation, Maintenance and Disposal Records Management Standard S1, 2010.*
- *Getting the most out of our knowledge and information*, UK Home Office, 2012.
- *Information and Records Management Standard*, Archives New Zealand, 2016.
- *Identifying Information Assets and Business Requirements*, The National Archives (UK), 2011.
- *Security Framework Policy,* UK Cabinet Office, 2014.
- *Better Information for Better Government,* UK Cabinet Office, 2017.
- *Information Management Policy Template,* National Archives of Australia.

For more information, please contact the Cayman Islands National Archive

Cayman Islands National Archive |P.O. Box 10160 |Grand Cayman KY1-1002 | CAYMAN ISLANDS Tel: +1 345 949 9809 | CINA@gov.ky