INFORMATION REGULATOR (SOUTH AFRICA)

Ensuring protection of your personal information and effective access to information

PROCEDURES FOR MAKING INFORMATION ELECTRONICALLY AVAILABLE

In terms of section 83(3)(a)(ii) of the Promotion of Access to Information Act 2 of 2000, as amended

MARCH 2022

CONTENTS

1. DEFINITION

1.1 **"Access"** means the right to, the opportunity to or the means of finding, using or retrieving information;

1.2 **"Accountability"** means the requirement to perform duties, including financial and operational responsibilities, in a manner that complies with legislation, policies, objectives and expected standards of conduct;

1.3 **"Appraisal"** means the process of determining the value of records for further use, for whatever purpose, and the length of time for which that value will continue. Also referred to as evaluation, review or selection. See also Functional appraisal;

1.4 **"Archives**" means **r**ecords, usually but not necessarily non-current records, of enduring value selected for permanent preservation or specific periods;

1.5 **"Archivist"** means **a** person professionally engaged in the management and preservation of archives.

1.6 **"Archival Institution"** means the agency responsible for selecting, acquiring, preserving, and making available archives;

1.7 **"Audit"** means the process of reviewing, verifying, evaluating and reporting on an organisation, system, process, project or product;

1.8 **"Audit Trail"** means, in relation to records and archives environment, a record showing the transactions within an information management system providing evidence of activities, such as who has accessed a computer system and when, what operations he or she has performed during a given time and the resulting changes to records or information;

1.9 **"Authenticity"** means, in relation to records and archives environment, the quality of being genuine and not corrupted or altered. The authenticity of a record is typically inferred from internal and external evidence, including the physical characteristics, structure, content and context of that record;

1.10 **"Automation"** means the use of machines or systems to perform tasks that might otherwise be performed or controlled manually;

1.11 **"Backup"** means the process of copying a computer file or collection of files to a second medium, usually on a diskette or magnetic tape, so that the data are safe in case the original file is damaged or lost. The resulting copy is also called a backup. Backup copies are usually stored on devices that can be removed from the computer and kept separately from the originals.

1.12 **"Classification"** is defined as the process of identifying and arranging records and archives in categories according to logically structured conventions, methods and procedural rules represented in a classification system;

1.13 **"Classification Scheme"** means a full representation of the business of an organisation, which systematically identifies and documents the organisation's activities and resulting records according to logically structured conventions, methods and procedural rules. Sometimes also referred to as a business classification scheme or file classification system. See also Retention and disposal schedule;

1.14 **"Classified Records"** means records that have been restricted in their circulation and access because they contain information that needs to be protected from unauthorised access. Classified records may bear security markings such as 'confidential,' 'secret' or 'top secret.' Sometimes also referred to as confidential or secret records;

1.15 **"Computer"** means any programmable machine or other device that can process information to produce a result;

1.16 **"Conversion"** means a process of changing records from one format to another;

1.17 **"Creation of Records"** means the first phase of a record's life cycle in which a record is made or received and then captured in a record-keeping system for action or for its evidentiary value. Also referred to as generation of records;

1.18 **"Data"** means electronic representations of information suitable for communication, interpretation and processing, generally by a computer system;

1.19 **''Data Subject''** means the person to whom personal information relates;

1.20 **"Description"** means, **i**n a records and archives environment, the process of capturing, analysing, organising and recording information that serves to identify, manage, locate and explain records and the contexts and records systems that produced them.

1.21 **"Destruction"** means process of eliminating or deleting records, through incineration, pulping, shredding, deletion or another method, so that it is impossible to reconstruct the records;

1.22 ***"*Digital Record"** means a record maintained in a coded numeric format that can only be accessed using a computer system that converts the numbers into text or images that can be comprehended by the human eye. Digital records include records stored in electronic and non-electronic formats such as optical disk;

1.23 **"Disposal"** means, in a records and archives environment, the actions taken to fulfil the requirements outlined in appraisal reports and retention and disposal schedules to retain, destroy or transfer records. Note that disposal is not synonymous with destruction, though destruction may be one example of disposal. Also known as disposition.

1.24 **"Disposal Date"** means, in a records and archives environment, the date on which actions specified in a retention and disposal schedule should be performed. Actions may include destruction, review, archival retention or transfer to storage;

1.25 **"Electronic Document"** means information recorded in a manner that requires a computer or other electronic device to display, interpret and process it. Electronic documents can include text, graphics or spread sheets, electronic mail and documents transmitted using electronic data interchange (EDI);

1.26 **"Electronic document management system (EDMS)**": means an electronic system or process – managed with the aid of computers and software – implemented in order to manage different kinds of documents in an organisation. Electronic document management systems may have limited records management functionality and may be combined with electronic records management systems;

1.27 **"Electronic Mail"** means also called email, a system for sending and receiving messages electronically over a computer network, such as between personal computers. The term also refers to the message or messages sent or received by such a system.

1.28 **"Electronic Information System"** is the organised collection, processing, transmission and dissemination of information according to defined procedures.

1.29 **"Electronic Record"** means a digital record that can be stored, transmitted or processed by a computer;

1.30 **"Electronic Records Management"** means the efficient management of records stored on computerised systems. The key to electronic records management is to be able to support such documents through their entire life cycle;

1.31 **"Electronic Records Management System (ERMS)"** means an electronic system or process – managed with the aid of computers and software – implemented in order to manage different kinds of records in an organisation. Electronic records management systems may also operate as electronic document management systems (EDMS). Note that electronic records management systems are not the same as electronic document management systems.

1.32 **"Electronic Record"** is any information that is recorded in machine readable form. Electronic records include numeric, graphic, audio, video, and textual information which is recorded or transmitted in analogue or digital form such as electronic spread sheets, word processing files, databases, electronic mail, instant messages, scanned images, digital photographs, and multimedia files;

1.33 **"Electronic Recordkeeping System"** is an automated information system for the organised collection, processing, transmission, and dissemination of information in accordance with defined procedures;

1.34 **"Evidence"** means**,** in a legal environment, information or proof admitted into judicial or legal proceedings and relevant to a specific case to establish an alleged or disputed fact;

1.35 **"File"** means, in a records and archives environment, an organised physical assembly of documents, usually held within a folder, that have been grouped together for current use or because they relate to the same subject, activity or transaction. A file is usually the basic unit within a record series. A file can be found in any format, but the term folder is more commonly used in digital record-keeping environments. **"File"** in a computer environment, means a logical assembly of data stored within a computer system. The term file is loosely used to describe a very wide range of assemblies of data from a single document to an entire database;

1.36 **"File Plan"** means, in a records and archives environment, a detailed list or inventory of the individual files or file categories within a classification scheme. A file plan allows for the systematic identification, filing and retrieval of records.

1.37 **"Folder"** means, in the desktop environment, an assembly of one or more documents grouped together because they relate to the same subject, activity or transaction;

1.38 **"Format"** means, in a computer environment, a structured means of encoding and storing digital information so that it can be interpreted by a software application;

1.39 **"Functional Appraisal"** means, in a records and archives environment, the process of assessing the enduring value of records by determining the functions of the body to be documented, identifying which offices or individuals created records in carrying out those functions and selecting the records that provide the most complete and concise documentation of the functions;

1.40 **"Group"** means, in a records and archives environment, the primary division in the arrangement of records and archives at the level of the independent originating organisation. Also known as archives group, fonds or record group;

1.41 **"Hard Drive"** means, in a computer environment, the storage area within the computer itself, where megabytes of space are available to store bits of information. Also known as a hard disk;

1.42 **"Hardware"** means, in a computer environment, the physical equipment required to create, use, manipulate, store and output electronic data;

1.43 **"Indexing"** means, in a records and archives environment, the process of establishing terms to describe and provide access to records and archives;

1.44 **"Information System",** means the combination of information, technology, processes and people brought together to support a given business objective;

1.45 **"Integrity"** means the quality of being whole and unaltered through loss, tampering or corruption;

1.46 **"Internet"** means a worldwide collection of computer networks that are linked together to exchange data and distribute processing tasks;

1.47 **"Intranet"** means an internal computer network that belongs to a particular organisation and is accessible only by that organisation's members;

1.48 **"Metadata"** means data describing the context, content and structure of records and their management through time. The preservation of the record with its associated metadata is necessary to maintain the integrity of the record. Types of metadata include technical / structural, administrative, descriptive, preservation and use;

1.49 **"Metadata for records"** means a structured or semi-structured information, which enables the creation, management, and use of records through time and within and across domains;

1.50 **"Microfilm"** means a process for photographing records and storing the images in miniaturised form on high-resolution film. Also refers to the product of the photographic process;

1.51 **"Migration"** means, **i**n a computer environment, the act of moving data or records in electronic form from one hardware or software system or configuration to another so that they may continue to be understandable and usable for as long as they are needed;

1.52 **"Organisations"** refers to public or private body and a **"body"** refers to public of private body;

1.53 **"Operating system"** means, in a computer environment, a collection of software that allows a computer to function;

1.54 **"PAIA"** means Promotion of Access to Information Act 2 of 2000; "POPIA" means the Protection of Personal Information Act 4 of 2013;

1.55 **"Preservation"** means, ***i***n a records and archives environment, the act of protecting records against damage or deterioration. The term is most often used to refer to the passive protection of archival material in which the item is not subject to any physical or chemical treatment;

1.56 **"Private Body"** means-

a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity;

b) a partnership which carries or has carried on any trade, business or profession; [or]

c) any former or existing juristic person; or

d) a political party,

but excludes a public body;

1.57 **"Public Records"** means, in a records and archives environment, records created or received and maintained in any public sector entities such as a government, public entities or state-owned enterprises;

1.58 **"Public Body"** means-

a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or

b) any other functionary or institution when-

(i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or

(ii) exercising a public power or performing a public function in terms of any legislation;

1.59 **"Record"** of, or in relation to, a public or private body, means any recorded information-

(a) regardless of form or medium;

(b) in the possession or under the control of that public or private body, respectively; and

(c) whether or not it was created by that public or private body, respectively.

1.60 **"Record keeping"** means the act of documenting an activity by creating, collecting or receiving records and ensuring that they are available, understandable and usable for as long as they are needed;

1.61 **"Record-Keeping System"** means an information system that captures, manages and provides access to records through time;

1.62 **"Records Management"** is a process of ensuring the proper creation, maintenance, use and disposal of records to achieve efficient, transparent and accountable governance. Records management includes processes for capturing and maintaining records as evidence of and information about business activities and transactions;

1.63 **"Records Manager"** means the person in charge of a records management unit or engaged in the records management profession;

1.64 **"Records System"** means an information system which captures, manages and provides access to records over time;

1.65 **"Register"** means a document, often a bound volume, in which standard data is captured about documents or records;

1.66 **"Reliability"** means, in a records and archives environment, the quality of being trustworthy; in reference to records, reliability is confirmed by ensuring that a record was created by a competent authority according to established processes and that the record contains all the necessary elements of an official record.

1.67 "**Repository"** means a storage facility, physical or electronic, where records are held for safekeeping. With reference to paper-based records, a repository is a building or part of a building in which records or archives are preserved and made available for consultation. Also known as an archival repository or archives. Note: To avoid confusion with the use of the term 'archives' to refer to records with on-going value, the term 'archives' is not used to refer to a repository.

1.68 **"Responsible Party"** means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;

1.69 **"Retention"** means the function of preserving and maintaining records for continuing use. Records may be retained in the system of origin, or transferred to a separate repository such as an offline system, records centre or archival institution;

1.70 **"Retention and disposal schedule"** means a document identifying the records of an organisation or administrative unit and specifying which records should be preserved permanently as archives and which can be destroyed after a certain period as obsolete or superseded. The retention and disposal schedule provides on-going authorisation for the transfer of records from offices to records centres, along with the destruction of obsolete records and the preservation of archival materials. Also known as a disposal list, disposition schedule, records schedule, retention schedule or transfer schedule;

1.71 **"Retention Period"** means***, i***n a records and archives environment, the length of time that records should be retained in an office or records centre before they are transferred to an archival institution or destroyed as obsolete. The retention

periods chosen for different records should be based on legislative or regulatory requirements as well as on administrative and operational requirements;

1.72 **"Scanning"** means, in a computer environment, the process of converting an image into a form that a computer can use;

1.73 **"Software"** means, in a computer environment, the automated instructions that allow a computer to manipulate data and execute particular functions or tasks.

1.74 **"Standard"** means a definition, format, specification, procedure or methodology that has been approved by a recognised standards organisation or is accepted as a *de facto* standard by an industry. Even if not formally recognised, a standard is normally considered an established or acknowledged model of authority or good practice.

1.75 **"Storage"** means, in a computer environment, the area within a computer system where data can be left on a longer-term basis while it is not needed for processing;

1.76 **"Tracking"** means, in a records and archives environment, the process of documenting the movements and uses of records so that their whereabouts are known at all times;

1.77 **"Transfer"** means, in a records and archives environment, the act of changing the location or ownership of, and / or responsibility for, records;

1.78 **"Unique identifier"** means in a records and archives environment, a reference number assigned to a record so that it can be distinguished from all other records;

2. BACKGROUND

2.1 Section 11 of PAIA provides a requester with a right of access to any records of a public body, whereas section 50 of PAIA provides for the right of access to records of a private body, if that record is required for the exercise or protection of any rights.

2.2 Section 23 of POPIA provides for the data subject's right to-

2.2.1 request a responsible party to confirm, free of charge, whether or not the responsible party holds personal information about the data subject; and

2.2.2 request from a responsible party the record or a description of the personal information about the data subject held by the responsible party, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information-

2.3 Access to information frequently means, in reality, access to records. Without documentary resources, public and private bodies cannot answer questions or provide information for the public. Since PAIA establishes time limits on the provision of information, finding information is critical to compliance with access legislation. Even without following a PAIA process, finding information in order to provide information to the public is and should be a central responsibility of any public and private body. Therefore, effective records management is an essential tool for ensuring that public and private bodies can find the right information at the right time, with minimal expense.

2.4 Just like physical records, electronic records need to be managed consistently. Effective management includes the following tasks:

2.4.1 setting up classification structures (to aid in filing records);

2.4.2 establishing retention and disposal rules (to determine how long to keep records and how to dispose of them);

2.4.3 assigning access permissions or security rights (to clarify who may use records);

2.4.4 determining whether a record is official (and so must be managed as part of a formal records management scheme) or transitory (and so should be removed from use as soon as it is no longer needed).

2.5 Unlike paper records, however, electronic records may be stored in various formats and on various media. For example, an electronic record may be saved as both a Word document and as a 'portable document format' or PDF (a format

that allows documents to be saved and exchanged over the Internet without alteration).

2.6 A difficulty with managing and using electronic records arises from the way in which they were created. Records created using instant messaging (IM), PDAs, and electronic mail (email) can be difficult to capture and preserve in an electronic record-keeping repository.

2.7 Another difficulty with preserving and protecting electronic records is the way in which they are created. For example, electronic mail can become like a conversation, with several messages building one on top of another. These 'threads,' as they are called, can become very long.

2.8 Detailed information regarding the management of electronic records is contained in the National Archives and Records Service's two publications Managing electronic records in governmental bodies: Policy, principles and requirements and managing electronic records in governmental bodies: Metadata requirements. Both publications are available on the National Archives and Records Service's website- http://www.nationalarchives.gov.za.

3. INTRODUCTION

3.1 The right of access to information is derived from section 32 of the Constitution which guarantees every person the right of access to any information held by the state and any information that is held by another person and that is required for the exercise or protection of any rights, regardless of when the record came into existence. The right is implemented through the enabling legislation listed in paragraph 6 below.

3.2 In order for information to be used, it has to be located elsewhere. Furthermore, personal, confidential or sensitive information needs to be protected so that people's individual rights to privacy are not violated. Protection is also needed in order not to circulate information that legitimately ought to be withheld. Of

particular concern are the grounds for refusal of access to records, contained in the PAIA[1].

3.3 PAIA was promulgated to give effect to the above-mentioned constitutional right of access to any information held by the state and any information that is held by another person and that is required for the exercise or protection of any rights. PAIA establishes voluntary and mandatory mechanisms or procedures to give effect to that right in a manner which enables persons to obtain access to records of public and private bodies as swiftly, inexpensively and effortlessly as reasonably possible.

3.4 In order to support the continuous flow of information, to ensure compliance with the regulatory environment and to promote transparency, accountability and effective governance of all public and private bodies, organisations should create and maintain authentic, reliable and usable records, and protect the integrity of those records for as long as required.

3.5 Organisations are increasingly reliant on information communications technology (ICT) as a crucial component of business operations and as a result, information or records are often partially or fully in electronic form.

3.6 The management of electronic records is a complex matter for which it is not possible to provide a simple set of guidelines applicable to all cases. However, the procedure set out in this document is intended to assist the creators and users of electronic records, information technology (IT) staff, records management (RM) staff, and managers in managing electronic records in an effective, cost-efficient manner that also accommodates their statutory obligation under the PAIA and any other legislation referred to in paragraph 7 below. The Guideline emphasises the crucial role of records maintenance and disposition in managing electronic records and is designed to be used in conjunction with any applicable legislation and policies.

[1] Section 33-46 and section 62-70 of PAIA

3.7 The international standard for records management, **ISO 15489-1[2],** establishes the core concepts and principles for the design, implementation and management of policy, information systems and processes allowing people, organisations, governments, private enterprises and collaborative coalitions to:

3.7.1 create and capture records to meet requirements for evidence of business activity; and

3.7.2 take appropriate action to protect the authenticity, reliability, integrity and usability of records, as well as their business context, and to identify requirements for their management over time

3.8 While the recommendations in this document reflect best practices, they are not meant to define mandatory standards for making information electronically available.

4. PURPOSE

The purpose of this document is to recommend the procedures in terms of which public and private bodies can make information electronically available in a manner which enables persons to obtain reasonable access to records swiftly, inexpensively and effortlessly.

5. OBJECTIVE

5.1 The main objective of these guidelines is to provide guidance to the public and private bodies in ensuring–

5.1.1 an efficient and systematic control of the creation, receipt, maintenance, management, use and disposition of records in an electronic environment, based on international standards ISO 15489; and

[2] ISO 15489 is an international standard for Records Management Systems (RMS), it was first published in 2001 and has since been revised and re-published, most recently in 2016. It is designed to help businesses and other organisations to manage their records to keep them reliable and up-to-date.

5.1.2 that their electronic records can be managed in order to make information readily available to users and to ensure authentic and reliable electronic records are protected for the long term; and

5.1.3 the reliability, usability, authenticity and integrity of their records; and

5.1.4 that authoritative evidence of business is created, captured, managed and made accessible to those who need it, for as long as it is required to enable the following:

5.1.4.1 improved transparency and accountability;

5.1.4.2 effective policy formation;

5.1.4.3 informed decision-making;

5.1.4.4 management of business risks;

5.1.4.5 continuity in the event of disaster;

5.1.4.6 the protection of rights and obligations of organisations and individuals;

5.1.4.7 protection and support in litigation;

5.1.4.8 compliance with legislation and regulations;

5.1.4.9 improved ability to demonstrate corporate responsibility, including meeting sustainability goals;

5.1.4.10 reduction of costs through greater business efficiency;

5.1.4.11 protection of intellectual property;

5.1.4.12 evidence-based research and development activities;

5.1.4.13 the formation of business, personal and cultural identity;

5.1.4.14 the protection of corporate, personal and collective memory.

6. STATUTORY AND REGULATORY FRAMEWORK

Electronic records, just like paper records, are subject to specific statutory and regulatory framework that the public and private bodies must understand and comply with. Efficient records management practises are imperative if a body wants to give effect to the provisions of the following legislations and records management standards-

6.1 **Promotion of Access to Information Act 2 of 2000**

6.1.1 The purpose of the Act is to promote transparency, accountability and effective governance by empowering and educating the public-

6.1.1.1 to understand and exercise their rights;

6.1.1.2 to understand the functions and operation of public bodies; and

6.1.1.3 to effectively scrutinize and participate in decision-making by public bodies that affects their rights.

6.1.2 The objects of this Act are to give effect to the constitutional right of access to any information held by the State; and any information that is held by another person and that is required for the exercise or protection of any rights.

6.1.3 This Act applies to-

(a) a record of a public body; and

(b) a record of a private body,

regardless of when the record came into existence.

6.1.4 Section 52A(1) of PAIA provides that “the head of a political party must create and keep records of any donation, make the records available and

keep the records for a period of at least five years after the records concerned have been created.

6.2 **The National Archives and Records Service of South Africa Act (Act. No. 43 of 1996 as amended)**

6.2.1 Section 13 of the Act contains specific provisions for efficient records management in governmental bodies. It provides for the National Archivist-

6.2.1.1 to determine which record keeping systems should be used by governmental bodies;

6.2.1.2 to authorize the disposal of public records or their transfer into archival custody; and

6.2.1.3 to determine the conditions–

6.2.1.3.1 according to which records may be microfilmed or electronically reproduced;

6.2.1.3.2 according to which electronic records systems should be managed.

6.2.2 The National Archives and Records Service, in terms of its statutory mandate, requires public bodies to put the necessary infrastructure, policies, strategies, procedures and systems in place to ensure that records in all formats are managed in an integrated manner. The National Archives and Records Service endorsed the SANS (ISO) 15489 Records Management Standard, SANS (ISO) 23081 Metadata for Records and SANS (ISO) 15801 Trustworthiness and Reliability of Records Stored Electronically.

6.2.3 The primary benchmark for creating and managing electronic records in office environments which is endorsed by the National Archives and Records Service is contained in the suite of publications; Principles and Functional Requirements for Records in Electronic Office Environments

adopted by the International Council on Archives in 2008. Module 2 of these publications, Guidelines and Functional Requirements for Electronic Records Management Systems relates to structured records systems such as those in which records are managed according to a file plan. A product that complies with these standards would possess the records management functionality required by the National Archives and Records Service.

6.3 **Protection of Personal Information Act, 2013**

6.3.1 POPIA prescribed conditions for the lawful processing of personal information by or for a responsible party and protect and regulate access to records involving specific individuals (personal information). in terms of POPIA, Individuals have a right to –

6.3.1.1 limit any access to, use of or dissemination of information directly related to them.

6.3.1.2 inspect and correct any information about them found in organisational records.

6.3.2 Section 14(1) of POPIA provides that records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless-

6.3.2.1 retention of the record is required or authorised by law;

6.3.2.2 the responsible party reasonably requires the record for lawful purposes related to its functions or activities;

6.3.2.3 retention of the record is required by a contract between the parties thereto; or

6.3.2.4 the data subject or a competent person where the data subject is a child has consented to the retention of the record.

6.3.3 Section 14(4) of POPI provides that a responsible party must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the responsible party is no longer authorised to retain the record in terms of subsection (1) or (2) thereof.

6.4 **The Public Finance Management Act (Act. No. 1 of 1999) and Municipal Finance Management Act (Act. No. 56 of 2003)**

6.4.1 The purposes of this Act are to regulate financial management in the public service and to prevent corruption, by ensuring that all governmental bodies manage their financial and other resources properly.

6.5 **The Promotion of Administrative Justice Act (Act. No. 3 of 2000)**

6.5.1 The purpose of this Act is to ensure that administrative action is lawful, reasonable and fair and properly documented.

6.5.2 The Promotion of Administrative Justice Act imposes a duty on the state to ensure that administrative action is lawful, reasonable and procedurally fair. Everyone whose rights have been adversely affected by administrative action has the right to be given written reasons for such an action. If an administrator to whom a request was made fails to furnish adequate reasons for an administrative action, because the history of that action was documented in e-mail messages or records that were destroyed, it could be presumed that the administrative action was taken without good reason. The administrator then runs the risk of legal action being taken against him/her or his/her organisation.

6.6 **The Electronic Communications and Transactions Act (Act. No. 25 of 2002)**

6.6.1 The purposes of this Act are to legalise electronic communications and transactions and to build trust in electronic records.

6.6.2 According to the Electronic Communications and Transactions Act, data messages are legally admissible records, provided that their authenticity and reliability as true evidence of a transaction can be proven beyond any

doubt. The evidential weight of electronic records (including e-mails) depends, amongst others, on the reliability of the manner in which the originator and the receiver managed the messages. Should bodies not have a properly enforced records management and e-mail policy and a reliable and secure record keeping system, bodies run the risk of the evidential weight of their electronic records (including e-mails) being diminished.

6.7 **ISO 15489 Information and documentation- Records management ("ISO 15489")**

6.7.1 ISO 15489 is an international standard for the management of business records, consisting of two (2) parts: Part 1: Concepts and principles and Part 2: Guidelines. ISO 15489 is the first standard devoted specifically to records management; providing an outline for comprehensive assessment of full and partial records management programmes.

6.7.2 ISO 15489 applies to the creation, capture and management of records regardless of structure or form, in all types of business and technological environments, over time. ISO 15489 has been developed with an acknowledgement of the following:

6.7.2.1 the roles of records as enablers of business activity and information assets;

6.7.2.2 increased opportunities for records use and re-use in the digital environment;

6.7.2.3 systems and rules for the creation, capture and management of records that need to extend beyond traditional organisational boundaries, such as in collaborative and multi-jurisdictional work environments;

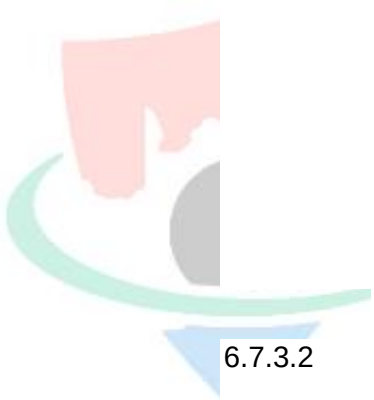
6.7.2.4 records controls that can be independent of other components of records systems;

6.7.2.5 the importance of recurrent analysis of business activity and context to identify what records need to be created and captured, and how they should be managed over time;

6.7.2.6 the importance of risk management in devising strategies for managing records and the management of records as a risk management strategy in itself.

6.7.3 **ISO/IEC 27001. *Information Technology — Security Techniques — Information Security Management Systems — Requirements***.

6.7.3.1 ISO/IEC 27001 is an international standard on how to manage information security. The standard was originally published jointly by the International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC) in 2005 and then revised in 2013. It details requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) – the aim of which is to help organisations make the information assets they hold more secure.



6.7.3.2 It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation.

6.7.4 **ISO 30300:2011, *Information and documentation – Management systems for records – Fundamentals and vocabulary*.**

6.7.4.1 The ISO 30300 series offers the methodology for a systematic approach to the creation and management of records, aligned with organisational objectives and strategies. Managing records using a management system for records (MSR) supports cost-effective operational processes, such as storage, information retrieval, information re-use. It prepares an organisation for the possibility of litigation or inquiry arising in the future and ensures that a thorough preparation for due diligence can be carried out.

6.7.5 The ISO 30300 series of International Standards focuses on the implementation and operation of an effective MSR to ensure that authoritative and reliable information about and evidence of business decisions and transactions is recorded, managed and made accessible to those who need it, and maintained for as long as it is required. This is fundamental and incontrovertible if the concerns of the public are to be addressed and current and future challenges are to be met.

6.8 Besides the above-mentioned legislation and standards, there are a number of other laws and records management standards that compel public and private bodies to manage information and records so that they are readily available and accessible when needed.

7. ELECTRONIC RECORDS MANAGEMENT POLICY

7.1 Public and private bodies (organisations) should define and document a policy for records management. The objective of the policy should be the creation and management of authentic, reliable and usable records that are capable of supporting business functions and activities for as long as they are required and accessible by the public.

7.2 Organisations should ensure that the policy is communicated and implemented at all levels in the organisation.

7.3 However, a policy statement on its own will not guarantee good records management. Critical to its success are endorsement, active and visible support by senior management, as well as allocation of the resources necessary for implementation.

7.4 A records management policy statement sets out what the organisation intends to do and sometimes includes an outline of the programme and procedures that will achieve those intentions. The policy statement should refer to other policies relating to information (e.g., those on information systems policy, information security or asset management), but should not seek to duplicate them. It should be supported by procedures and guidelines, planning and strategy statements,

disposition authorities, and other documents that together make up the records management regime.

7.5 A record should correctly reflect what was communicated or decided or what action was taken. Records management policies, procedures and practices should lead to authoritative records that have the following characteristics:

7.5.1 **Authenticity**

An authentic record is one that can be proven to-

7.5.1.1 be what it purports to be

7.5.1.2 be dully issued by an authorised person or agency;

7.5.1.3 have been created or sent by the person purported to have created or sent it;

7.5.1.4 have been created or sent at the time purported;

7.5.1.5 be verified by testing physical and formal characteristics of a record

7.5.2 **Reliability**

7.5.2.1 A reliable record is one that is capable of standing for the facts to which it attests and 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.

7.5.2.2 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

7.5.3 **Integrity**

7.5.3.1 The integrity of a record refers to it being complete and preserved without any alteration that would impair its use as an authentic record/document. It is necessary that a record be protected against unauthorised alteration. Records management policies and 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 authorized, and who is authorized to make them. Any authorized annotation, addition or deletion to a record should be explicitly indicated and traceable.

7.5.3.2 If the information is going to be used in a legal proceeding, organisations must be able to identify who has had access to a particular record at any given time from collection to creation of the evidence copy, to present the information as evidence. The evidentiary weighting of records will be substantially reduced if the chain of custody cannot be adequately established or is discredited.

7.5.3.3 In order to ensure integrity of records, organisation must make sure that the documents, information or data must be; -

7.5.3.1 accurate and free from error or defect;

7.5.3.2 consistent with a standard, rule or policy;

7.5.3.3 unmodified and never changed in form, meaning or character; and

7.5.3.4 consistent and uniform over its life cycle.

7.5.4 **Usability**

7.5.4.1 A useable record is one that can be located, retrieved, presented and interpreted. It should be directly connected to the business activity or transaction that produced it.

7.5.4.2 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.

8. AREAS OF RESPONSIBILITY

8.1 Broad responsibility of information officers

8.1.1 The information officers are ultimately responsible for the records management practices of the organisations under their possession and control.

8.1.2 The responsibilities of the information officers of public bodies in terms of the National Archives and Records Service of South Africa Act, 1996 are set out in the National Archives and Records Service of South Africa Regulations and the Records Management Policy Manual.

8.2 Records Manager

8.2.1 Information officers of the public and private bodies should designate staff members at the senior management level to whom they can delegate the responsibility to ensure that sound records management practices are implemented and maintained. These officials are the records managers of the bodies.

8.3 Users

8.3.1 Sound records management is a collective responsibility which all members of staff have an equal obligation to maintain.

8.3.2 All users should be aware of the policies, procedures, and tools for managing records and they should be capable of applying them consistently to all records.

8.3.3 In order to file documents into the filing system and to protect the records against any loss and damage and for purposes of being responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, there must be full co-operation of the users.

9. CREATING ELECTRONIC INFORMATION SYSTEMS

9.1 Electronic recordkeeping systems must have accurately documented policies, assigned responsibilities, and formal methodologies for their management. Electronic recordkeeping systems must meet the following criteria:

9.1.1 **Consistent**: process information in a manner that assures the records they create is credible.

9.1.2 **Complete**: contain content, structure, and context generated by the transaction they document.

9.1.3 **Accurate:** quality controlled at input to ensure the information in the system correctly reflects what was communicated in the transaction.

9.1.4 **Preserved**: records must continue to reflect content, structure, and context within any system by which the records are retained over time.

9.2 For electronic information systems that produce, use, or store data files, disposition instructions for the data shall be incorporated into the system's design.

9.3 Public and private bodies shall maintain adequate technical documentation for each electronic information system, including documentation of system design, implementation, use, and migration. The following documentation is required:

9.3.1 Narrative description of the system;

9.3.2 Physical and technical characteristics of the records, including a record layout that describes each field including its name, size, starting or relative position, and description of the form of the data (such as alphabetic, decimal, or numeric), or a data dictionary or the equivalent information associated with a database management system including a description of the relationship between data elements in data bases; and

9.3.3 Other technical information required to access or processes the records.

9.4 Organisations must implement the following procedures to enhance the legal admissibility of electronic records:

9.4.1 Documents with similar kinds of records generated and stored electronically are created by the same processes each time and have a standardised retrieval process.

9.4.2 Substantiate that security procedures prevent unauthorized additions, modifications, or deletions of records and ensure protection of the system against such problems as power interruptions.

9.4.3 Identify the electronic media on which records are stored throughout their life cycle, the maximum time span that records remain on each storage media, and the official retention requirements.

9.5 Recordkeeping systems should meet the legal and administrative requirements, national and international standards, and best practices for recordkeeping in an electronic environment. Electronic recordkeeping systems should also include an approved disposition plan.

9.6 In an electronic business environment, adequate records will not be captured and retained unless the system is properly designed. It is important to note that media

for storing digital data, and also formatting the data, are subject to change. For example, a significant number of documents archived by an organisation over the past decade may now be largely illegible and incomprehensible because of damage to storage media or because the older file formats are incompatible with newer, currently used formats. The public and private bodies are required to implement and maintain Integrated Document and Records Management Systems that provide, as a minimum, the following records management functionality:

9.6.1 managing a functional subject file plan according to which records are filed;

9.6.2 managing e-mail as records;

9.6.3 managing websites as records;

9.6.4 maintaining the relationships between records and files, and between file series and the file plan;

9.6.5 identifying records that are due for disposal and managing the disposal process;

9.6.6 associating the contextual and structural data within a document;

9.6.7 constructing and managing audit trails;

9.6.8 managing record version control;

9.6.9 managing the integrity and reliability of records once they have been declared as such;

9.6.10 managing records in all formats in an integrated manner; and

10. MANAGING ELECTRONIC RECORDS

10.1 Traditionally, organisation have considered the evidentiary implications of electronic documents only when they are required for litigation or by regulatory bodies (such as the Regulator), or when forensic practitioners have focused on

collecting IT evidence as artifacts of an investigation. However, successful management of IT evidence is much broader than a mere post-mortem activity, and the IT evidence must be managed continuously throughout the records life cycle.

10.2 Sometimes digital records need to be archived for a certain period of time, so that, if necessary, they can be presented during the court process. With the current pace of technological development, it is very likely that problems with outdated storage media or formats of data can make the process of returning data very expensive. This can be because of the need to complete the conversion of all data to new media as technology develops or because of the need to keep the old equipment and software.

10.3 Guidelines for managing all electronic records-

10.3.1 Electronic records should be reliably and securely maintained;

10.3.2 Electronic records should be retained or disposed of in accordance with authorized and approved records retention schedules;

10.3.3 Work processes and associated business procedures and tools should support the creation and management of electronic records;

10.3.4 Electronic records should be inviolate and secure;

10.3.5 Electronic records should be preserved without loss of any vital information for as long as required by law and policy;

10.3.6 Electronic records should be accessible and retrievable in a timely manner throughout their retention period; and

10.3.7 Access to electronic records should be controlled according to well-defined criteria;

10.4 Not many organisations have the capacity to implement fully automated Integrated Document and Records Management Systems. This does not however mean that they should not manage their electronic records. If these records are created to

aid in decision-making and to perform transactions that support the organisation's activities, public and private bodies are responsible for the proper management of those records. If records generated in such an environment are not managed properly it can lead to the possible loss of, damage to or unauthorised destruction of records.

10.5 To enhance their accountability, public and private bodies should ensure that, even without the benefit of an Integrated Document and Records Management System, they exercise effective records management.

10.6 There are four common ways of creating, using and storing documents in an electronic environment:

10.6.1 in personal computers, where individuals control the creation and use of the records;

10.6.2 in shared computer servers, where individuals control the creation of records but share those records with others in the organisation;

10.6.3 in shared servers with centralised control, where all individuals adhere to established procedures for creating and managing records; and

10.6.4 in shared servers using electronic document or records management software, where control over the creation and use of records is strongly regulated.

10.7 **Managing Records in Shared Computer Drives**

10.7.1 In most organisations, users have access to a series of networked computer drives, where they create, store and access corporate documents and share information through Intranet or Internet sites. Typically, an organisation maintains the following types of computer drives**:**

10.7.1.1 a corporate-wide shared drive, containing documents relevant to the whole organisation;

10.7.1.2 a branch or divisional shared drive, containing documents relevant to a single organisational unit; and

10.7.1.3 a personal drive containing documents relevant only to the individual.

10.7.2 Using shared network drives has many advantages. For example, staff can-

10.7.2.1 place documents on a shared drive and let people know it is there (called 'publish and point') rather than duplicate documents multiple times;

10.7.2.2 develop logical and useful filing structures for shared drives;

10.7.2.3 develop and adhere to common terminology;

10.7.2.4 establish control over the creation of folders within computer systems;

10.7.2.5 develop 'good housekeeping' practices for synchronising the creation, use and disposal of documents.

10.7.3 Of course, the successful use of shared drives depends on the creation of and adherence to clear and use policies for managing electronic documents.

10.8 **Adopting a Publish and Point Approach**

10.8.1 A 'publish and point' policy is a method of controlling the duplication of a document while it is being widely circulated. Instead of attaching the document to an email message, which sends each recipient an individual copy, a read-only version of the document is placed on a shared drive – in other words, it is published – and a pointer or shortcut is emailed to alert intended recipients. Recipients can then retrieve the document from the shared drive as required. A publish and point policy-

10.8.1.1 encourages a culture of sharing documents as organisational resources, rather than retaining them as individually owned items;

10.8.1.2 encourages users to think more carefully about the most appropriate method for distributing information;

10.8.1.3 reduces the number of working copies of records in individual folders. A publish and point policy will tend to decrease the requirements for individual document storage, but it may increase the network traffic and may require more storage space in shared computer servers.

10.9 Establishing General Filing Structures

10.9.1 When a significant number of documents are stored on a shared network drive, a basic general filing structure should be established. If a division or branch (or a specific project) has developed its own filing structures, these structures should aim to conform to the principles of a general filing structure in order to prevent divergent practices and application.

10.9.2 End users should also be encouraged to use consistent filing structures in their own group and personal workspaces, not just when filing into shared drives. This consistency will help the organisation coordinate the creation, use and retention of working papers and final documents and will ease retrieval and access of information throughout the institution.

10.10 Configuring a Secure Record Drive

10.10.1 A secure record drive is a shared network drive that has been configured in such a way as to prevent the amendment or unauthorised deletion of documents on the drive. With such a mechanism in place, organisations are more likely to consider the electronic document to be the official corporate record, even though a paper copy may also exist. Any records considered official and final should be stored separately from transitory or non-official electronic documents, and the organisation should

establish clear definitions about who has the right to access, add records to or delete records from the drive.

10.10.2 When establishing a separate storage location for official records, consider the following suggestions-

10.10.2.1 Before establishing a separate storage area, assess the risks involved with this approach and clearly identify the types of documents which it may be acceptable to manage in this way. Remember that a secure drive does not provide the same level of security as a fully managed ERMS;

10.10.2.2 Use a separate logical hard drive with read-only settings to prevent anyone from making changes to documents that have been saved to the drive;

10.10.2.3 Ensure that users can read and create documents but that they cannot replace existing documents, with edited versions.

10.10.2.4 Ensure appropriate backup and recovery procedures and maintain necessary levels of security at the operating system level.

10.10.3 Although separate storage areas can provide reasonable sound storage of documents in the short term, there will be challenges with migrating material to a full ERMS later. For instance, a Microsoft Windows directory structure does not easily provide document and folder level metadata that will support a structured migration to an ERMS. Although migration can be achieved, it may be a relatively expensive process. Research is critical before decisions are made and new systems implemented.

10.11 **Understanding and Applying Naming Conventions**

10.11.1 Standardising the way in which folders and documents are named can dramatically improve access to electronic records. Applying naming conventions results in-

10.11.1.1 better access to and retrieval of electronic documents;

10.11.1.2 improved sorting of documents into logical sequences by version number or date;

10.11.1.3 easier identification of documents in lists or directories;

10.11.1.4 better management of different versions of documents.

10.11.2 Essentially, naming conventions serve two related functions:

10.11.2.1 Consistent naming of folders or documents brings related items together under a common label; and

10.11.2.2 Consistent naming also distinguishes similar items by naming each in a consistent, logical and predictable way.

10.12 **Standardising Terms**

10.12.1 Since every organisation's core business is and ought to be different from the business of every other organisation, it is not possible to 'cut and paste' classification schemes from one unit to another. It is necessary to analyse each organisation's duties and responsibilities and determine an appropriate classification scheme accordingly. A useful tool for improving consistency and streamlining the classification process is a functions thesaurus, which helps to standardise the terms used to refer to different functions and activities.

10.12.2 A functions thesaurus is an alphabetical list of preferred terms for use in a classification scheme or other records management tools. The terms are linked together by their different relationships, so that the user can review terms related to a particular function or activity and determine the best term to label it when categorising its records. Thus, the thesaurus helps support standardisation and consistency by ensuring that the same terms are used when representing the same type of function or activity.

10.12.3 For example, an organisation involved with the development and delivery of workshops could refer to its work using words such as ‘workshops,’ ‘training,’ or ‘education.’ Which is the best term? What about other terms, such as ‘schooling,’ ‘teaching,’ ‘guidance,’ or ‘instruction’? A thesaurus helps determine which term should be used in a particular instance and recommend against the use of other terms if they were not considered appropriate.

10.12.4 A thesaurus can also support the standardisation of terms representing common activities or types of records that may appear across the organisation. Selecting one term and using it consistently has many benefits, including-

10.12.4.1 encouraging common use of language for similar work;

10.12.4.2 maximising the retrieval of information using search features in records management software;

10.12.4.3 supporting decisions about whether common types of records may or may not warrant similar retention periods.

10.12.5 The development of a thesaurus of terms is one way to standardise the use of names and terms.

10.13 Creating File or Document Names

10.13.1 Creating understandable and logical document or file names is essential to easy and quick retrieval of records. At a minimum, all document names should include a title, a version number and a date.

10.13.2 Don’t forget these tips when developing naming conventions-

10.13.2.1 Remember that nothing comes before something (for example, when sorting records in an electronic filing system, the term ‘Policy’ would come before the phrase ‘Policy Directives’);

10.13.2.2 Similarly, using zeros can ensure documents sort in proper numeric order so that they are displayed in order on the computer screen (for instance, 10 will come before 9 but 09 will come before 010).

10.13.2.3 If retaining specific reference numbers is important, it is possible to add those to the metadata for the record, so that they can be searched and retrieved through the computer system.

10.13.2.4 Standard terms and forms of name should be used wherever it is sensible to do so. In particular, this can apply to the names of people or organisations, the names or projects and activities and logical document types. When choosing between the full spelling of a name and an acronym, it is important to be consistent; do not use the full name sometimes and the acronym at other time. For example,

a) Choose between e-government and electronic government.

b) Use accepted acronyms, such as DOH instead of Department of Home Affairs. Do not use Dept. of Home Affairs, D-home-affairs, or dept-h-a.

c) Use standard terms for document types, such as agenda, letter, minutes, project report, memo and so on.

d) If the author's name is captured in the metadata (and it should be) then it usually does not need to be repeated in the document title. If using personal names, decide whether to use forename then surname or surname then forename: Jason Smith or Smith Jason. Do not use the two orders interchangeably.

e) When a date is necessary in the document or folder title, order the elements so that they display chronologically, for example in a YYYYMMDD pattern. Months spelled alphabetically do not file in chronological order

10.13.2.5 Document titles should contain enough information to identify them if they become detached from the correct folder. Also important is to ensure that the relationship between individual documents and the folders in which they are stored is maintained in a meaningful fashion within the record-keeping structure.

10.14 Controlling Versions of Documents

10.14.1 Consistent naming rules can link different versions of the same document, by including a version number as part of the title. This approach will also help to provide an audit trail for future tracking of document development, but the success of this method depends on accurate and careful naming and tracking of versions. There is a danger of inconsistency if different users access and update different versions of a document without coordinating their efforts. As a result, different versions may exist throughout the organisation. Well-developed and robust procedures are important for the control of document versions in a multi-user environment.

10.14.2 A first task is to establish procedures for when to call a document a new version or when to save it with the same title as the previous edition. Remember that what constitutes a substantive change depends on the business context of the work being performed. For instance, all versions of legislation under development may need to be kept, but only the final version of an administrative memo may be worth keeping.

10.14.3 A common method for version control numbering is to use the ordinal number (1, 2, 3, etc.) for major version changes and the decimal number for minor changes, as in: ver. 0.5; ver. 1.0; or ver. 2.7. A

version 1.0 normally denotes a first document version given wider circulation.

10.15 Using computer software to standardise records creation

10.15.1 While computer software packages such as Microsoft Word advertise that they can capture metadata and apply file names and titles consistently, the reality is that the computerised features in such software are usually neither useful enough nor flexible enough to suit the specific needs of a particular organisation. For example, there is a feature in Microsoft software called 'Document Properties' that allows users to capture metadata about the document being created: the software will capture information such as author, title, keyword 'tags' and date. There are advantages to using a Document Properties feature, such as the following-

10.15.1.1 Standard key metadata terms will always accompany the document.

10.15.1.2 The history of the creation and use of the document will be documented over time.

10.15.2 However, there are also disadvantages, as shown below:

10.15.2.1 Requiring staff to fill in Document Properties metadata leads to more work before records can be closed and filed.

10.15.2.2 The metadata can be misleading, especially if document production is shared: for example, the Author field may take the last-named editor even though several people have worked on the document.

10.15.2.3 In practice, no one may bother to use or maintain the metadata gathered using Document Properties.

10.16 **Controlling Dates**

10.16.1 In some applications, such as Microsoft applications, it is possible to insert a generic date field, which can be updated automatically by the computer application each time the document is saved or opened.

10.16.2 This feature is convenient when used carefully, but it will provide false information if it is used indiscriminately, particularly where different types of date are not clearly labelled and identified.

10.16.3 The best course of action is to turn off the automatic date function and require staff members to insert date information manually.

10.17 **Saving Electronic Documents**

10.17.1 In order to provide on-going access to records, it is important to define standard formats in which documents should be saved, particularly if many different software applications are in use or many people need to access and use records. It is always preferable to limit the number of formats used as much as possible, to reduce the difficulty of providing access or preserving records in the future. There are basic options for saving documents, as outlined below-

10.17.1.1 One choice is to standardise on an exchange format, when multiple application versions are in use. For example, you can use the Microsoft version of RTF, by saving all corporate documents in an RTF format (which the application can be set to do automatically). These documents will be accessible by different application versions (e.g. MS Word 97 and MS Word 95) and by other word processors; for further modification or manipulation but some formatting information may be lost in certain circumstances.

10.17.1.2 Another choice is to standardise on a distribution format, which is most appropriate once documents are finalised and the content will not change. For example, a PDF

rendition of a document converts documents so that they can be read but not revised. However, it is necessary to have the appropriate Acrobat software for creating PDFs. This option is unlikely to be cost-effective in an organisation with a large number of direct users, and access to the documents is best provided through a centralised storage function, which may not be available in smaller organisations.

10.17.2 In order to determine the most appropriate method for saving or sharing documents, it is necessary not just to select the easiest or most accessible option but to research different approaches thoroughly.

10.18 **Collecting Metadata**

10.18.1 There are two options for collecting metadata when creating and using electronic records in the office environment. Both options may be relevant for different types of records and both may be used together, depending on the nature of the computer systems in place.

10.18.2 Metadata can be captured automatically by computer systems or it can be gathered systematically by having the creators and users of records complete forms and templates.

10.18.3 Metadata may also be added by records managers and archivists as records are transferred throughout the record-keeping system. In recent years, work has been underway to develop software that will capture metadata after the fact using what are called ‘utility programmes.’ Generally, though, both manual and computerised approaches will be used to capture metadata.

10.18.4 Much of the technical metadata related to a digital resource is automatically captured, such as file format (such as ‘doc’ or ‘pdf’) or software application and version (such as Adobe 8) are captured automatically. Metadata that is entered by a user may include descriptive elements such as links to related documents, custodial

history (changes in ownership of a document, particularly as a result of reorganisation of an institution) and title.

10.18.5 Metadata elements may also require modification by users if the software captures the information automatically. For instance, in most word processing applications, the title of the document is automatically captured by the computer programme. In these instances, the first line of the document becomes the title, but this string of words may not be useful or meaningful. Consequently, the user will need to modify the title manually to something more appropriate.

10.18.6 **Issues to Consider when Collecting Metadata**

10.18.6.1 When developing a process for capturing metadata, it is important to consider the following issues-

10.18.6.1.1 The greater the amount of metadata attached to a record, the higher the potential cost for storing and managing the metadata and the record.

10.18.6.1.2 The poorer the quality of the metadata, the harder it is to manage, locate, retrieve and access electronic information.

10.18.6.1.3 Entering complex metadata efficiently, accurately, and consistently can be costly, time consuming and error-prone, leading to inaccuracies and inconsistencies. Vigilance is required to ensure quality information is gathered.

10.18.6.2 Manual capture of metadata can lead to variations, depending on the interpretations made by different people during the process. To avoid variations, it is important to-

10.18.6.2.1 use naming conventions consistently;

10.18.6.2.2 use metadata that are meaningful to the users and the organisation;

10.18.6.2.3 train staff thoroughly and monitor their work regularly;

10.18.6.2.4 focus on capturing metadata schema that is useful for the organisation's business processes and do not attempt to create elaborate systems if they are not required.

10.18.7 Another difficult challenge with capturing metadata is getting staff members to comply with the process. Many users do not want to enter information into computer screens, considering it a poor use of their often very limited time. It is important to convince them that managing metadata effectively will help improve their business operations, maybe even saving them time in the long run.

10.18.8 With the development of more sophisticated electronic records and document management systems, the capture of essential metadata is becoming easier, as the software applications automatically gather a great deal of important information automatically.

10.19 **Synchronising Computers**

10.19.1 With the increasing use of laptops, handheld computers and personal digital assistant devices (PDA's), it is common to find that documents have been duplicated in different computer locations. If procedures for synchronising computers are not established, important documents may be lost, potentially conflicting versions may be retained and confusion can result.

10.19.2 It is important, therefore, to establish procedures for managing different technologies, including-

10.19.2.1 maintaining a filing structure on a laptop that is consistent with the structure used on the desktop;

10.19.2.2 developing a disciplined approach to updating document versions;

10.19.2.3 nominating a single storage location for documents in development, to hold the primary version and later updates.

10.19.3 File synchronisation facilities such as Microsoft Windows Briefcase, which keeps track of changes to particular files, can help to control duplication, as long as the software is used properly. Windows is not designed to handle file conflicts easily, and it is not a substitute for effective procedures, particularly in cases where several members of a work team are working on the same documents.

10.19.4 A similar synchronisation facility is often used with Microsoft Outlook and Microsoft Exchange to synchronise folders between the email mailbox of a laptop and the user's primary network mailbox. Many people use this facility to create emails using the local laptop copy, and these emails are later uploaded to the main mailbox for dispatch. The synchronisation facility harmonises changes in both main and local mailbox versions. Potential difficulties can arise where two separate copies of a message – a local copy and a main copy – have been edited separately, resulting in conflicting versions. It is essential to establish procedures for uploading locally made changes to the main mailbox before editing or transmitting main mailbox versions of messages.

10.20 **Managing Electronic Mail**

10.20.1 Electronic mail (email) messages should always be treated as potential corporate records of the organisation. More and more departmental business is conducted by email, replacing the conventional memo and, increasingly, the formal letter. To manage email effectively, it is necessary to establish policies and procedures for-

10.20.1.1 clarifying which emails should be kept;

10.20.1.2 managing messages within the email system;

10.20.1.3 managing emails in shared drive folders when necessary;

10.20.1.4 managing the composition of emails and the exchange of emails (as threads develop);

10.20.1.5 helping individuals to manage their own mailbox.

10.20.2 Valuable records can be lost if email is not managed effectively, but it can be difficult to establish firm control over email creation and use. Since email is not a record series but is instead a mechanism for the transmission of information, an electronic mail system cannot be scheduled in its entirety; individual decisions have to be made about which emails to keep and which to destroy. As well, retention of messages depends on their content and context, and both content and context differ depending on whether the message has been sent or received, how an email thread develops and who is responsible for what part of the communication process.

10.20.3 Therefore, email policies are essential to guiding users about which types of email messages should be kept in the short-, medium- and long term. Policies should cover-

10.20.3.1 whether and when messages sent and messages received should be retained;

10.20.3.2 how to manage email threads;

10.20.3.3 whether and when drafts of emails should be retained;

10.20.3.4 who will have access to different types of emails.

10.20.4 In addition, organisational policies should emphasise-

10.20.4.1 the fact that any email message relating to departmental business may be considered an official record;

10.20.4.2 the importance of taking care with language used when composing emails;

10.20.4.3 the importance of protecting personal privacy when communicating via email;

10.20.4.4 the importance of avoiding any inappropriate content in email messages.

10.20.5 In an organisation that does not have a computerised ERMS system in place, there are three main approaches to managing email records:

10.20.5.1 by adopting a 'print-to-paper' policy

10.20.5.1.1 An organisation may adopt a policy of printing all emails and filing them in the paper filing system. There are drawbacks to this approach. For example, documents are often not actually printed and placed on a paper file, because this task is seen as increasingly burdensome by the end user at the desktop. As well, it may not be possible to print all the metadata that exist within the email system. On the other hand, the electronic version of the document may not be consistently managed either, and emails may be stored in a variety of locations and under different names, with no guarantee of accuracy and therefore with limited access.

10.20.5.2 by managing emails within the email system itself

10.20.5.2.1 Retaining emails within the organisation's email system is sometimes the easiest way to preserve them, since the person responsible – the office worker at the desktop – does not need to undertake many

actions beyond just creating, sending, receiving and/or filing the message. However, if the user is storing emails in personal folders, then access is limited to that person only, or his or her designate, and so the record is out of the reach of the organisation as a whole. On the other hand, if messages are stored in a work team space or shared folder, access is improved but controls over naming conventions are critical. If emails are kept in public folders, then security issues need to be addressed as some messages may contain confidential information.

10.20.5.2.2 The advantage of managing messages within the email system is that all metadata relevant to the record is captured and preserved, and the messages are kept within a familiar environment, making it easier for staff to comply with filing requirements. There are disadvantages, however. For instance, email messages in an email system are not integrated with other relevant documents; as a result, parallel filing structures will develop, making it hard to find information and avoid duplication. Still, managing emails within the existing email system is a good interim solution, since staff can develop filing practices that will be useful in the future, if the organisation develops an ERMS system.

10.20.5.3 by saving messages to a shared drive.

10.20.5.3.1 Saving messages to a shared drive helps bring together all documents and messages relevant to a theme or activity in the same folder, which significantly improves corporate access to the organisation's records. This approach is close to the way in which email messages would be managed in an ERMS system. Unfortunately, the process of manually saving emails into a shared drive is often cumbersome and staff members are not always willing to comply. It is also important to clarify who is responsible for saving emails, since many messages are circulated widely within an organisation but only one or two people may have official responsibility for the business tasks associated with the message.

10.20.5.3.2 When saving emails into a shared drive, they can be saved in various formats. A .msg format is convenient within the Microsoft Outlook environment, but it is a proprietary format and therefore it may be more difficult to migrate documents to other systems later, if the commercial software is not available. An .rtf format is a fairly standard exchange format, which will embed any attachments within the message body, but saving .rtf files takes more disk space and so can become more costly to maintain. Saving emails in .html format is not recommended; as mentioned earlier, the syntax used for .html may contain proprietary elements and access the information might be limited if commercial software is not available.

10.20.5.3.3 When establishing procedures to save emails on a shared drive, it is important to decide whether to save attachments with the message or separately. There are differing opinions on the question but the general approach is to save the message and the attachments together when any significant information related to the topic is contained in the message itself. If the message is just a container for the attachment however – such as a message written to forward a report with the text 'here it is,' – then it is recommended that the attachment be saved and the email itself destroyed.

10.20.5.3.4 When saving email messages outside of the email system, transmission data, showing fields such as date of sending and receipt, recipients, subject title, should always be saved with the message text. However, as with printing to paper, some other metadata may very well be lost. As well, encryption tools should not be used when saving messages to a shared corporate drive, or access will be hindered.

11. MANAGING RECORDS IN A HYBRID ENVIRONMENT

11.1 As is a common cause that many organisations will continue to create both paper and electronic records as a normal part of their daily activities. Managing this hybrid record-keeping environment is normal and expected; it is unlikely that a purely electronic records framework will be found anywhere in the world in the near future. In order to co-ordinate the management of both paper and electronic records in a hybrid environment, the following few suggestions should be considered-

11.1.1 Linking Electronic and Paper Filing Systems

A shared network drive can usually be configured to reflect the paper filing structure so that electronic documents are stored in a manner comparable to their paper counterparts. This approach may be achievable by building a hierarchical 'folder within a folder' structure using Microsoft Windows, to simulate the structure of a paper file plan. As you investigate how to link electronic and paper filing systems, consider the following points-

11.1.1.1 There is little point in building a paper-based structure in electronic folder form if the structure does not work well in the paper environment. Often, the implementation of an ERMS forces an organisation to rethink its paper filing systems, but even before an ERMS is contemplated it is worth looking closely at existing filing systems before copying them.

11.1.1.2 Alphabetical folder titles are generally more usable in the electronic environment than numerical schemes. Using both letters and numbers together will produce very long folder titles.

11.1.1.3 Paper filing systems tend to use long names. In a Microsoft Windows environment, some of the file directory information might not be seen on the computer screen, making it difficult to identify and access records. As well, the longer the folder or file name, the more chance that it will exceed the limit allowed in a software application, making the document essentially unusable.

11.1.1.4 If paper and electronic filing systems are co-ordinated, it is important to establish clear directions about who can create paper or electronic folders and who is responsible for ensuring that both the paper and electronic systems remain co-ordinated. Allowing everyone to create their own folders and files will eventually result in a breakdown of the systems.

11.1.2 Scanning Paper Records

11.1.2.1 It is sometimes desirable to scan paper records and retain the electronic copies as part of the electronic record-keeping system. Many issues need to be considered when developing a scanning programme, not the least of which is ensuring the quality, authenticity, and integrity of the record in electronic form. But first, the organisation needs to decide why it wants to scan records and preserve them digitally. *Is the goal to save storage space? To save money? To provide improved access to information?* The reasons for digitisation will determine what will be digitised and how.

11.1.2.2 The following questions need to be answered when planning a digitisation initiative-

11.1.2.2.1 Is the goal to save space? If so, the organisation should first ensure it has implemented an effective records management programme, one that moves records through the life cycle and destroys or transfers records regularly.

11.1.2.2.2 Is the goal to provide improved access? If so, the organisation should ensure that the records to be digitised are worthy of long-term retention; if they are only going to be kept another few years, the cost of scanning will likely far outweigh any storage costs incurred. The organisation may also want to make any scanned text searchable by including optical character recognition (OCR) as part of the scanning process.

11.1.2.2.3 Whether the purpose is to save space or improve access, the organisation must determine how the scanned records need to be 'profiled' so that they can be found. What naming convention will be used? What other data for accessing the records

will be needed? How much of this data can be captured automatically and how much will have to be input manually?

11.1.2.2.4 Are there any legal concerns associated with replacing paper records with electronic ones? The organisation needs to be able to confirm the authenticity and integrity of the scanned copies, and there may be legitimate reasons for retaining the originals instead of or as well as providing electronic versions.

11.1.2.2.5 Are the paper-based originals suitable for scanning? If the quality of the electronic product is not high enough, the original may need to be retained for evidential or information purposes. It is important to test the scanning process before committing to widespread scanning projects, in case some records are not suitable and must be retained in their original form.

11.1.2.2.6 What format should the electronic copies be kept in? If the integrity of the copies is to be maintained, they could be saved as PDF files or other unchangeable formats. But if the organisation wishes to use, alter or manipulate the records, then it may want to save them in a word processing format that allows changes. However, the organisation then needs to assess the implications for the authenticity and integrity of the original evidence.

11.1.2.2.7 How long electronic and paper copies should be retained? Once a record is scanned, the organisation needs to clarify if the original will be destroyed immediately or if it will be kept for a certain time, if not permanently. The organisation

will also have to determine which version will be considered the official record, if both are to be retained. Legal restrictions on the destruction of records must be identified so that the organisation does not breach any laws in the process of digitising records.

11.1.2.2.8 How will the electronic record be made accessible? There is an increased risk of violating privacy and confidentiality when making any records available electronically. The organisation needs to assess the privacy concerns and the access procedures to be used before deciding if it is appropriate to scan certain records in order to make them more widely available in an online environment.

11.1.2.3 If a scanning programme is established, the organisation needs to establish policies and procedures on how it will be managed. These policies and procedures should confirm that the organisation is complying with legislative and other requirements to ensure that the digitisation process results in authentic and trustworthy documents. Quality control and regular monitoring of the scanning programme are important to confirm that the process is operating as it should. The organisation may need to create a certification process, wherein certificates are scanned along with the originals confirming the technical specifications followed and attesting to the fact that the procedures are up to expected standards.

12. DEVELOPING CLASSIFICATION SCHEMES

12.1 The task of classification is to identify different categories of business functions and activities, and the records generated as a result of the work performed, and group those records into logical units in order to facilitate access, storage and disposal.

12.2 The classification scheme is one of the important foundations for any electronic or paper records management programme: it is the central tool used to describe, categorise and control records. The classification scheme should process series or groups of records efficiently and effectively so that retention and disposition rules can be applied consistently; when used in an electronic environment, a further goal is to allow for the comprehensive computerised search and retrieval of both the record and the metadata.

12.3 Classification enables the creation of a structured file plan so that everyone in the organisation can easily identify the one logical and unique physical or intellectual 'place' in which to file records. Classification organises records into mutually exclusive categories so that there can be no doubt about the appropriate place for an individual item. If records are filed logically, information can be retrieved by anyone at any time according to a consistent set of rules and guidelines.

12.4 The great advantage of managing electronic records is that a strong classification scheme can be supported by computerised indexing tools, allowing users to retrieve records not only based on their functional purpose but also by names, dates, keywords or types of documents.

12.5 As people have started using computer technologies, they have become used to creating, managing, and filing their electronic documents themselves. Even though well-structured file plans may exist for the organisation's paper records, office workers rarely adopt that plan for the management of their electronic files. Consequently, electronic documents are often created according to individual preferences, making it harder to find, use and manage them.

12.6 One of the benefits of automation is the flexibility it provides for creating and revising records and for searching for and retrieving information easily and quickly. One of the difficulties, however, is that if an electronic record is not stored in a logical place, and if the terms used to search for it do not relate to actual words or phrases within or associated with the document, it is virtually impossible to find. Therefore, classification of records becomes even more important when dealing with electronic information.

12.7 Scheduling, review, preservation, and destruction decisions should be applied to records in one group in the same way at the same time. It is particularly important

to ensure all records are managed consistently to ensure the government adheres to records or access legislation; it is a serious breach of the law to find that a record that ought to have been kept has been destroyed or a record that should have been destroyed was kept in error. Managing records in the aggregate is the only efficient and effective way to ensure consistency. An electronic records management system that does not allow for the creation and maintenance of file and folder structures will not serve essential records management requirements well.

12.8 The reality is that most organisations will have to manage both electronic and hard copy records. It is therefore critical to have a classification system that functions perfectly in a hybrid environment: that is, a record-keeping environment containing both paper and electronic records. A classification scheme needs to support the storage and retrieval of records that will be created and kept in different physical locations: some on computer servers or storage devices, others in filing cabinets or storage boxes. An effective classification scheme will function efficiently in this hybrid environment.

12.9 A well-structured classification scheme, whether for manual or electronic records, will-

12.9.1 suit the particular needs of the organisation it serves;

12.9.2 enable unique identifiers (titles and/or reference numbers or codes) to be assigned to each item that requires classification, in order to facilitate management and retrieval;

12.9.3 be fully documented so that all the rules and structures used to classify records are consistent;

12.9.4 will be flexible, to allow for changes in the nature of work and records over time;

12.9.5 will be reviewed and revised on an on-going basis, in order to ensure it is always current and relevant.

12.10 Some of the important qualities of an effective classification system, whether for electronic or paper records, are outlined as follows-

12.10.1 **An effective classification system will support business or organisational requirements**

12.10.1.1 It will suit the organisation it serves and support decision-making and the activities of the organisation.

12.10.1.2 It will match users' needs.

12.10.1.3 It will be cost effective.

12.10.1.4 It will be properly resourced, with adequate equipment, funds or staff.

12.10.1.5 It will not be dependent on outside resources for operational requirements.

12.10.2 A classification system will be easy to understand, use and maintain-

12.10.2.1 It will be understood by records staff and users.

12.10.2.2 It will be independent of human memory.

12.10.2.3 It will use simple processes.

12.10.2.4 It will inspire confidence in operators and users.

12.10.3 A classification system will be precise-

12.10.3.1 It will minimise doubt about where to file records.

12.10.3.2 It will allow the quick identification and retrieval of files.

12.10.4 A classification system will be complete and comprehensive-

12.10.4.1 It will cover all the files that need to be included.

12.10.4.2 It will be capable of including files that may be created in future.

12.10.4.3 It will be flexible and allow for expansion, contraction or reorganisation.

12.10.5 A classification system will be backed up by a procedures manual and associated training materials-

12.10.5.1 It will be clearly and comprehensively documented.

12.10.5.2 Its scope and use will be explained in easy-to-follow steps.

12.10.5.3 It will provide master copies of all forms, with completed examples.

12.10.5.4 It will be supported by training programmes.

12.10.5.5 It will be supported by professional advice or guidance.

12.10.6 A classification system will be easily computerised-

It will be adaptable for use in electronic records management systems.

13. GOOD ELECTRONIC RECORDS HOUSEKEEPING

13.1 Consistent and on-going management of both shared and personal drives, and paper filing systems, is essential to maintaining the long-term viability of records.

13.2 Staff members should be trained to review their records periodically and remove any non-official materials along with unnecessary duplications; ideally, they should be encouraged not to capture non-official materials in the record-keeping system in the first place. This housekeeping work is external to the application of formal retention and disposal schedules and so becomes an individual responsibility. The goal should be to reduce unneeded duplication of records while still ensuring good access to information for business purposes.

13.3 Procedures should be established to clean up unnecessary duplicates, working copies that are no longer required and documents with no continuing value. Staff should be reminded regularly to review their filing systems, their local drives, personal workspaces and other paper or electronic work areas and reduce as much clutter as possible. They should also be reminded regularly not to use their local or personal drives for the long-term storage of official corporate documents.

13.4 **Each public and private body should implement and maintain the following record control mechanisms-**

13.4.1 **Register of files opened**, which contains a description and opening dates of all files that were opened according to the subject provisions in the filing system.

13.4.2 **Register of disposal authorities**, if any, which contains copies of all disposal authorities issued by the National Archives and Records Service, to that specific body.

13.4.3 **Destruction register**, which contains information on the year in which non-archival records are due for destruction.

14. APPRAISAL AND DISPOSAL OF ELECTRONIC RECORDS

14.1 The appraisal and disposal of electronic records are essential to the sustainability of a quality ERM programme. Preserving valuable records and destroying obsolete ones ensures that only necessary records are retained and saves the organisation time and money. While the focus in this unit is on the appraisal of electronic records, the purpose of appraisal remains the same for all records no matter their medium. Appraisal involves determining what records exist or will be

created; who creates them and why; how they relate to the organisation's business functions; and how, when and by whom they are used, and then deciding which records have enduring value and which can be removed once their immediate usefulness is at an end.

14.2 **When to Appraise?**

14.2.1 Traditionally, paper records were appraised long after they had been created, used and stored. Indeed, it was common to wait 30 to 50 years or more after records were created before deciding whether or not to retain them permanently. Fortunately, paper-based records are 'neglect tolerant' and can, within reason, withstand the environmental dangers associated with storage, such as fluctuating temperature and humidity, damage from dust or vermin and excessive light levels, for limited periods.

14.2.2 Electronic records are unlikely to survive neglect, and it is not possible to wait decades before deciding what to keep and what to destroy. The technology used to create the records may become obsolete in one or two years, if not sooner, and so it is imperative that decisions be made about which electronic records should be kept at the time they are created, if not before.

14.2.3 Ideally, therefore, appraisal and disposal activities should be built into the normal practice of records management, becoming as routine a procedure as possible. Non-systematic appraisal work – perhaps done in response to poorly planned office moves or the last-minute rescue of records from garbage bins – will interfere with the quality of the appraisal and will, therefore, hinder the work of preserving quality records. The success of appraisal of electronic records depends on the active involvement of records professionals. As noted above, a records retention and disposal schedule should be created as a central tool in managing the on-going disposal of electronic or paper records. However, it is often necessary to carry out a one-time appraisal exercise for a select group of records or for all the records in the organisation, either to clear up a backlog of records or to lay the groundwork for the creation of a formal electronic records management programme.

14.2.4 The best method for appraisal of records – both paper and electronic – in a modern office environment is a macro-appraisal approach, based on an analysis of the functions and activities of the creating body, a process called 'functional appraisal. Functional appraisal involves assessing the enduring value of records by determining the functions of the body to be documented, identifying who created records in order to carry out those functions and then selecting the records that provide the most complete and concise documentation of those functions. Functional appraisal is currently considered the best way to appraise large volumes of records, no matter the medium in which they were created, in a way that minimises potential bias and encourages the preservation of those records that provide the most complete and concise picture of significant organisational functions.

14.3 **Appraisal as a Risk Management Activity**

14.3.1 If records creators and archival institutions had all the time, money, employees and space in the universe, then no records would ever need to be destroyed. However, this is not the reality, and so archival institutions, in collaboration with record creators, need to make rational and informed decisions about what to keep and what to remove. Please refer to section 14 of POPIA in so far as retention of records are concerned.

14.3.2 The greatest risk electronic records face is the risk of being altered, manipulated, overwritten or destroyed, resulting in an inauthentic and unreliable record or, worse, no record at all. This risk is compounded by the prohibitive cost of maintaining all the technology and expertise needed to retain electronic records in their original form. The changes in computers and information systems happen far too quickly to allow organisations the luxury of keeping 'old' computers just so they can access electronic records in their original configuration, especially when a large percentage of those records are not worth preserving for the long term.

14.4 **Who is Responsible for Appraisal?**

14.4.1 Developing clearly defined responsibilities for appraisal and disposal activities is essential to ensuring successful records management, regardless of the form of the records. Traditionally, appraisal and disposal activities were divided, with the records manager determining the time frame for semi-active retention and the archivist determining the final disposal. Now, in the electronic records environment, it is practical for the records manager, archivist, information technology specialist and records creator to work as a team, in order to bring a range of expertise to the process of deciding which records need to be kept and which can be destroyed.

14.4.1.1 The records creator brings knowledge of the day-to-day use of records and their importance to the organisation's business.

14.4.1.2 The information technology specialist can advise on changes to electronic systems and best practices in IT operations.

14.4.1.3 The records manager supports the on-going evidential and informational needs of the organisation and can balance the user's needs for records against the resources available in order to make solid judgements about records retention.

14.4.1.4 Archivists have the long-term management of the records in mind and are responsible for ensuring authentic and reliable records remain accessible over the long term.

14.4.1.5 Lawyers, auditors, compliance specialists and other subject experts can also contribute important insights during the process of appraisal.

14.4.2 These stakeholders – along with any other appropriate representatives of the organisation – should be involved in any appraisal exercise, and their different responsibilities and areas of authority should be clearly defined and formalised in appraisal policies. The archivist may be the primary

appraisal specialist, but he or she should draw on the expertise of others in the organisation throughout the process.

14.5 Documenting Appraisal and Disposal

14.5.1 No matter who undertakes appraisal and disposal work, documenting all decisions and actions is essential to ensure the organisation remains answerable for its actions and to guarantee that detailed information is available about all work performed. Documentation provides audit trails for important decisions, which render governments accountable to the citizens they serve. As well, future records professionals may need to revisit appraisal decisions, and documentation is essential to reconstruct the reasoning and logic used in making disposal decisions.

14.5.2 Documentation of appraisal and disposal actions can also be valuable for other purposes, such as the creation of archival descriptions and finding aids, and the development or revisions of records classification schemes. Documentation also provides analysis and information related to the authenticity and preservation of electronic records that may be critical for their long-term care.

14.5.3 The following are different types of documentation that can be generated as part of an accountable and transparent appraisal process-

14.5.3.1 **Appraisal Step 1: Conducting Research-** Any appraisal decision must be based on solid information and research. A critical first step is to gather and analyse as much information as possible about the records' context of creation and use, as well as information about the records themselves.

14.5.3.2 **Documentation from Step 1-** Following is the key documentation resulting from the research conducted in Step 1-

14.5.3.2.1 A compilation of all contextual information gathered from the records creator and from outside sources.

14.5.3.2.2 A technical analysis.

14.5.3.2.3 Notes, transcriptions or audio / video recordings of interviews with staff.

14.5.3.3 **Appraisal Step 2: Determining Value-** The appraisal team uses the information and research gathered in Step 1 to determine the value of the records throughout the life cycle: in the active, semi-active and inactive phases, in order to determine how long the records should be retained. Once the value of the records is assessed, those precise retention periods can be assigned and a retention and disposal schedule can be developed, using the records classification scheme as the basis.

14.5.3.4 **Assessing the Business and Accountability Value of Electronic Records-** In assessing the value of records to determine their retention for business and accountability purposes, the appraisal team may ask questions such as:

14.5.3.4.1 Why and how does the records creator use the electronic records?

14.5.3.4.2 How long does the records creator need the records in order to conduct business?

14.5.3.4.3 What legal requirements must the record creator meet regarding the protection or use of electronic records?

14.5.3.4.4 Might the records be needed for audit, quality control or other evaluation purposes? If so, for how long might such needs continue?

NOTE: The answers to these questions will come from a careful analysis of the organisation's legal, financial and

business requirements as well as a review of the organisation's current information needs.

14.5.3.5 **Assessing the Archival Value of Electronic Records -** Besides meeting the legal or operational needs of the organisation, a decision needs to be made about whether records need to be preserved for posterity. Questions to ask include-

14.5.3.5.1 Are the electronic records valuable enough to society to have enduring value?

14.5.3.5.2 What will be the final disposition action for electronic records?

14.5.3.5.3 Will archives be sent to an archival institution for preservation or preserved internally using the organisation's own facilities and resources?

14.5.3.5.4 How will obsolete records be destroyed?

NOTE: The challenge with electronic records preservation is ensuring the technological capacity is available to carry out the decisions and protect the records for the long term.

14.5.3.6 **Determining Authenticity and Integrity-** The appraisal of electronic records must include an assessment of their present authenticity and an analysis of whether and how they can be preserved with their authenticity intact. Electronic records are more easily altered, manipulated and overwritten than records on traditional media, and therefore their integrity may be compromised. The integrity of electronic records is most at risk when they are transmitted between people, organisations or software systems. An electronic records system that does not capture adequate metadata and other important components of the electronic record will put the

authenticity of the records at risk and will not allow the records in the system to stand as reliable evidence of the body's work.

NOTE: If, however, all the required elements of the record exist, the archivist may then make a strong presumption of authenticity. Therefore, identifying the required elements of the electronic record and discovering how they are expressed in the electronic system is critical when assessing the authenticity of the electronic records.

14.5.3.7 **Assessing Electronic Records Systems**-

14.5.3.7.1 A high presumption of integrity for electronic records can be made if certain conditions exist in the system used to create and house the records, including clearly defined and fully implemented procedures for-

a) controlling access to records;

b) preventing the loss or corruption of records;

c) preventing media deterioration or technological obsolescence; and

d) carrying out regular audits of the electronic system.

14.5.3.7.2 When assessing the context of the electronic records system, the appraisal team should attempt to answer the following questions-

a) How is access to the system controlled?

b) Who has or had access and what level of access did they have?

c) Does the electronic records system use passwords and other means to control access?

d) What are the file formats used? Are the files formats still compatible with the current technological environment or do records exist in file formats that are obsolete or unsupported?

e) What storage media are used, where is the storage media located and is this location secure?

f) Have the electronic records been transmitted from another body or outside organisation, and how?

g) Has there been any other break or change in the chain of custody? How and why?

h) Have the records been migrated into a new hardware or software environment? When and how?

i) Are the records inactive and, if so, how long have they been so?

NOTE: The answers to these questions will help the archivist assess the organisational and technological context surrounding the records and help reveal whether the records can be considered authentic and reliable.

14.5.3.8 **Determining the Feasibility of Preservation**

14.5.3.8.1 When considering the archival value of electronic records, another question the appraisal team

must consider is whether it is feasible to preserve the records for the long term. Preservation is expensive and time consuming, and it is an on-going responsibility – as technologies change, preservation approaches must also change.

14.5.3.8.2 To determine the feasibility of preserving electronic records, the appraisal team can use the information about the technological context of the electronic records that was gathered in Step 1 to analyse the current hardware and software environment. During a technical analysis, the archivist must examine how the records are created in the computer and how they are saved.

14.5.3.8.3 Once this research is completed, the archivist must then determine whether the organisation – either the creating body or the archival institution – has the ability to preserve the electronic records. Questions to ask include-

a) Does the organisation have the financial resources needed?

b) Does the organisation have the appropriate technical equipment?

c) Does the organisation have the technical expertise and knowledge?

d) Is the organisation committed to maintaining these records indefinitely?

14.5.3.9 **Documentation from Step 2-** Following is the key documentation resulting from the research conducted in Step 2-

14.5.3.9.1 A technical analysis detailing the components of the electronic records and the controls needed to ensure that electronic records will not be tampered with or otherwise altered. The technical analysis also includes analysis of the formats of the records and identifies possible preservation and / or access formats.

14.5.3.9.2 A list of the types of hardware and software needed to access and view the electronic records.

14.5.3.9.3 Information about the archival institution's ability to preserve electronic records, such as annual work budgets, staff profiles, equipment lists, information from upper management and similar documentation.

14.5.3.10 **Appraisal Step 3: Making an Appraisal Decision**

14.5.3.10.1 After assessing the value of the electronic records being appraised, at the point when they are being considered for transfer a decision needs to be made either to preserve the records or destroy them. The options are as follows:

a) If the records are no longer found to have enduring value, they will be destroyed.

b) If the records are found to have enduring value, and if it is reasonable to assume that they are authentic and if long-term preservation is feasible, the records will be preserved.

c) If the records are found to have enduring value, but there is some question of whether or not they are authentic, or if

preserving the records will require extraordinary efforts or expenditures, the appraisal decision must be made through a case-by-case analysis.

NOTE: In addition to making the final appraisal decision, the archivist must specifically identify, in writing, which electronic records and other components in the electronic system (such as metadata profiles or other information) must be transferred along with the records, and which electronic records and other components must be disposed of. It is imperative that those components needed in order to implement disposal be clearly identified. The same authorisation is required if the records are to be destroyed.

14.6 **Monitoring Appraisal Decisions**

14.6.1 It is vitally important that archivists and other records professionals be involved in the development and implementation of electronic records systems as well as in the appraisal of electronic records.

14.6.2 Appraised records should be monitored for the following situations-

14.6.2.1 Unexpected changes in business processes can affect how electronic records are used by action officers;

14.6.2.2 Minor changes in the software and hardware environment made after the system has been implemented may affect authenticity or alter preservation options; and

14.6.2.3 Major changes to the software and hardware environment may place records at risk of loss or damage.

14.7 14.6.4 Whilst it is not possible to demonstrate the authenticity of records or assess the potential for preservation before the records have been created, monitoring operations may lead not only to small changes in appraisal documentation, but

also, sometimes, to more significant changes in the overall appraisal decision.

Confidentiality

14.7.1 Identify confidential records maintained on the system.

14.7.2 Confidential or exempt information must be masked when it is necessary to deliver censored copies.

14.7.3 Access to confidential records should be restricted based on security level and defined in user security permissions.

15. CREATING A RETENTION AND DISPOSAL SCHEDULE

15.1 Section 14(1) of POPIA provides that, subject to subsections (2) and (3), records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless-

15.1.1 retention of the record is required or authorised by law.

15.1.2 the responsible party reasonably requires the record for lawful purposes related to its functions or activities.

15.1.3 retention of the record is required by a contract between the parties thereto; or

15.1.4 the data subject or a competent person where the data subject is a child has consented to the retention of the record.

15.2 Section 14(3) of POPIA provides that a responsible party that has used a record of personal information of a data subject to make a decision about the data subject, must-

15.2.1 retain the record for such period as may be required or prescribed by law or a code of conduct; or

15.2.2 if there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

15.3 A valuable tool for records management is the records retention and disposal schedule, which identifies how long records within different series should be retained and whether they should ultimately be kept for their enduring value or destroyed as obsolete. The retention and disposal schedule is a central document in any records management programme, whether for paper or electronic records. It is generated out of the process of appraisal and draws on the information provided in a classification scheme. Disposal schedules have the following four functions-

15.3.1 They identify all the records of a body, irrespective of medium and format, including those created in the private offices of ministers or senior officials, as well as confidential and secret records created elsewhere.

15.3.2 They document decisions about the length of time records need to be retained because of their continuing utility to the creating body (retention periods).

15.3.3 They document decisions about the appropriate disposal action to be taken at the end of retention periods (such as destruction or retention as archives); and

15.3.4 They confirm that disposal actions have been authorised by appropriate agencies.

15.4 The core function of a retention schedule is the date or time period for retention. This information triggers the ultimate disposal of the records. For example, the retention rule for a series of electronic payment vouchers might indicate a destruction date of six years after the end of the fiscal year in which the payment voucher was issued. This metadata should break down into the following three metadata elements required in order to execute the retention and disposal rule-

15.4.1 The retention trigger, which might be the end of the fiscal year in which the voucher was set aside. The retention trigger is the date that the system uses to begin 'counting down' to the end of the retention period.

15.4.2 The retention period, the retention period is the amount of time before the final disposal action.

15.4.3 The final disposal action, either to retain records permanently or destroy them: in this case the disposal action might be to destroy the records.

15.5 In electronic records systems, retention and disposal metadata can be applied to a whole series of records by linking retention information to the classification scheme. This functionality is one reason archivists and other records professionals need to be involved at an early stage in the development of electronic records systems, so that they can support the development of classification schemes and the retention and disposal of metadata before records are created within the system, saving time and effort and improving the management of and access to records.

15.6 Some retention triggers do not always work for all records in an electronic records environment. For example, trigger dates that are defined by chronological time and expressed as a date within the year (e.g., 31 December 2007) are easily implemented into electronic systems because they can reference the time/date clock function of most computer systems. However, retention triggers not defined by chronological time, such as those defined by events, can be more difficult to implement. For example, event triggers such as 'end of project,' 'after application acceptance,' or 'after termination of lease' cannot always be calculated or entered automatically. Instead, someone must manually enter the information in the metadata profile of the record.

15.7 Additionally, a record may be created in the electronic system before the exact date when the event trigger is known. For example, electronic records created for a construction project might be scheduled for disposal ten years after the end of the project. When the records are initially set aside in the electronic system, the records creator may not know precisely when the construction project will end, making it impossible to computerise the retention process. In such instances, event triggers should be monitored by a responsible party outside the electronic

environment to ensure that the retention and disposal metadata is complete and that the electronic system can execute the disposal command using accurate metadata.

15.8 For computer systems that do not have records retention and disposal functions, the archivist or records manager will need to create procedures for the scheduled disposition of records. Using the electronic payment voucher introduced above as an example, the business processes for disposing of those documents would generally proceed as follows:

15.8.1 The series of electronic payment vouchers are assigned a retention period of six years after the fiscal year in which the vouchers were issued. They are deemed to have no enduring value after that retention period has expired.

15.8.2 Six years later, the records manager identifies the payment vouchers that were set aside six years before.

15.8.3 Once the records have been identified, the records manager confirms that that correct records have been identified and oversees their destruction through complete deletion from the system.

16. DESTROYING OR DELETING OR DE-IDENTIFYING RECORD

16.1 If records have been appraised as having no long-term enduring value, then they may be destroyed at the end of their life and the physical destruction of records should be carried out by methods appropriate to their level of confidentiality.

16.2 In accordance with section 14(4) and (5) of POPIA, a responsible party must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the responsible party is no longer authorised to retain the record. Section 14(5) of POPIA requires that the destruction or deletion of a record of personal information, referred to in paragraph 22.2 above, must be done in a manner that prevents its reconstruction in an intelligible form.

16.3 For paper records, destruction means to physically destroy the record, by shredding, burning or otherwise obliterating the records' medium. Records in

electronic form can also be destroyed by reformatting or rewriting, if it can be guaranteed that the reformatting cannot be reversed. Deleting instructions is not sufficient to ensure that all system pointers to the data incorporated in the system software have also been destroyed. Backups containing generations of system data also need to be reformatted or rewritten before effective destruction of electronic information is complete. It is not simply enough to erase the records from a computer directory. It may also be necessary to identify and destroy the components and metadata associated with the electronic record. Technical expertise may be required to ensure this destruction is carried out.

16.4 It is also necessary to maintain an audit trail of the destruction process. While the technology available in different organisations will vary, the general principle of destruction remains the same: every attempt should be made to ensure that data cannot be recovered by reasonable efforts. The security or sensitivity of the information should be used to determine what constitutes 'reasonable. The only exception is the documentation generated by the destruction process itself; that documentation – which should include a description of the records destroyed and the means by which they were destroyed – should be retained as evidence of the act of destruction.

16.5 The steps involved in destroying electronic records are as listed below-

16.5.1 Identify records that have no enduring value.

16.5.2 Confirm that the records are going to be destroyed or otherwise disposed of according to the formal agreement between the preserver and the records creator.

16.5.3 If the records are to be destroyed, destroy them completely.

16.5.4 Analyse the steps taken to ensure compliance with all requirements.

16.5.5 Complete the destruction report and submit it to the appropriate authorities within the organisation.

17. TRANSFERRING RECORDS

17.1 If records are appraised as having long-term enduring value, then the records should be transferred to the chosen archival facility, whether that is a separate archival institution or a permanent storage facility within the organisation. The appraisal research and technical analysis conducted in Step 2 and the formal agreement on the terms and conditions of transfer in Step 3 will indicate how the records should be transferred into the custody of the archival institution and in which format(s).

17.2 The assessment of preservation requirements conducted in Step 2 will provide valuable information about how the records need to be prepared for transfer. It is a good practice to transfer electronic records in both their original, native format and, if necessary, as a reformatted version (a copy). Keep in mind that the technical analysis may have identified the need for two reformatted versions: one for long-term preservation and another for access purposes.

17.3 The process of reformatting electronic records for the purpose of transfer must be fully documented in a transfer report. The transfer report should also include the following information, which will be critical for carrying out later work with the records, such as arranging and describing archives, preserving files and providing access to records:

17.3.1 a list of the electronic records selected for transfer.

17.3.2 information about the electronic records' native format(s).

17.3.3 a description of the preservation and / or access formats used; and

17.3.4 information about how the electronic records were copied and reformatted.

17.4 The archives must maintain the record of what was done to the records, if and how they were altered and what elements or components made up the electronic records before they were transferred. In general, the steps in the transfer process are as follows-

17.4.1 Identify records that have enduring value and will be transferred to the archival institution.

17.4.2 Determine the format in which those records will be transferred: options include the native format, another preservation format or an access format.

17.4.3 Copy and, if necessary, reformat the records to be transferred.

17.4.4 Prepare transfer documentation, including a detailed list of records to be transferred; information about file formats used; and any technical documentation needed to support access and preservation.

17.4.5 Transfer records and documentation to archival custody.

17.4.6 Confirm the successful transfer of records; and

17.4.7 Delete the records from the source system.

17.5 Continuing Retention

17.5.1 Records identified for continuing retention need to be stored in environments conducive to their long-term preservation. Preservation strategies for records, especially electronic records, may be selected based on their ability to maintain the accessibility, integrity and authenticity of the record over time, as well as for their cost-effectiveness.

17.5.2 Preservation strategies can include copying, conversion and migration of records:

17.5.2.1 Copying is the production of an identical copy within the same type of medium (paper/microfilm/electronic), e.g., from paper to paper, microfilm to microfilm, or the production of backup copies of electronic records (which can also be made on a different kind of electronic medium).

17.5.2.2 Conversion involves a change of the record's format but ensures that the record retains the identical primary information (content). Examples include microfilming of paper records, imaging and change of character sets.

17.5.2.3 Migration involves a set of organised tasks designed to periodically transfer digital material from one hardware/ software configuration to another, or from one generation of technology to another. The purpose of migration is to preserve the integrity of the records and to retain the ability for clients to retrieve, display and otherwise use them. Migration may occur when hardware and/or software become obsolete, or it may be used to move electronic records from one file format to another.

17.5.3 Information may be stored for a considerable length of time and for longer than the lifetime of the current technology. Thus, to ensure the integrity of stored information, it is important to plan from the outset that the information may be subject to a migration process. Such a process may involve a change of media, computer hardware or software.

17.5.4 As a rule of thumb, a storage media migration process will occur approximately every five years. A reliable methodology for dealing with this potential problem is to ensure that data files are stored in an industry standard format, or that viewers for each stored format are maintained. It is also recommended that a restricted number of formats are used for long-term storage, to reduce future storage migration issues.

17.5.5 When making provisions for migrating data files, it is important to include all relevant metadata, including index data and audit trails. These additional data should also be migrated to the new technology without loss of integrity. Records, including audit trails, should be kept of any migration process to which stored data have been subjected, to allow the integrity of the data to be demonstrated beyond any reasonable doubt at any time in the future.

17.5.6 As new technologies become available, other methods may be used to retain electronic records for long periods.

17.5.7 Where records are transferred to an external storage provider or an external archives authority, documentation that outlines continuing obligations to maintain security measures on integrity and confidentiality of the records and manage them appropriately should be formally

established by agreement between the custodian(s) and the transferring party.

18. DEVELOPING ACCESS TO INFORMATION POLICIES IN AN ELECTRONIC ENVIRONMENT

18.1 Providing public access to and protecting the privacy of information in electronic records can be more challenging than providing access to information in traditional paper records. The value of records changes over time, and public interest in different subjects rises and falls depending on political, social or other imperatives. As well, finding and retrieving electronic records can take place quickly – if adequate records management controls are in place – but at the same time it is more difficult to ensure that electronic records are not at risk of inappropriate disclosure, unwanted duplication or inadvertent destruction. The following are some of the issues that might need to be considered in order to provide public access to records in an electronic framework-

18.1.1 How will access be affected by any changes in the technologies used to create, manage and store electronic records?

18.1.2 When providing access to electronic records, how will the organisation distinguish between multiple copies of or versions of one 'record'? Will it decide that one version should be considered the appropriate record for public disclosure, or give access to all versions?

18.1.3 What hardware and software will be needed to provide access to electronic records, and will new systems or approaches be required to provide public access as distinguished from organisation-wide access to electronic information?

18.1.4 How will the organisation protect the authenticity of electronic records when providing access? Will records be 'certified' as traditional paper records often are?

18.1.5 Will the organisation charge for access to electronic records? What about charges for providing print copies of records?

18.1.6 Will the organisation allow the public to file access requests electronically?

18.1.7 What records will be required to document and track such access requests?

18.1.8 Will the organisation establish an online repository of already public information, including records that have been released through previous access requests, in order to provide a proactive approach to access instead of a reactive one?

18.1.9 What costs would be associated with establishing and maintaining such a resource?

18.2 Even though it is increasingly accepted that the public in general have a right of access to records of the public and private bodies, it is necessary to develop specific policies that regulate access to information. Any policies related to access need to be established within the legislative framework outlined in paragraph 7 above.

18.3 The primary purpose of access to information policies is to articulate who can have access to which records, when and how. But access policies also help an organisation enhance its accountability, promote transparency and nurture public trust.

18.4 Before developing an access to information policy, an organisation should undertake the following three specific tasks in order to able to identify and assess different risks, establish procedures for managing the access process and assign responsibilities for further action. -

18.4.1 Identify the regulatory framework affecting access and privacy, including identifying all the laws and regulations (including those described above) that may have a bearing on any decisions about providing access to information;

18.4.2 Conduct a records survey and/or business process analysis, to identify all the records created by the body and identify those that need to be managed in order to ensure appropriate access is provided; and

18.4.3 Carry out a risk assessment to determine the dangers of inadvertently providing or denying access to information that ought to be managed differently.

18.5 All access policies should include the following key components:

18.5.1 statements outlining the objectives, purpose and scope of the policy;

18.5.2 information about related laws, regulations or policies that may affect access provisions in the organisation or business area;

18.5.3 statement of how the organisation intends to respond to those laws and -regulations;

18.5.4 identification of who is responsible for overseeing the overall implementation of the policy and/or fulfilling the detailed requirements of the policy; and

18.5.5 an explanation of the sanctions in place for non-compliance with the policy.

18.6 **Implementing Access to information Policies**

18.6.1 Once access policies are established, the organisation should review all documents created to ensure they are comprehensive and accurate, and then the organisation might consider testing the policy against actual or fictitious access requests to see if any policy-related concerns emerge. For the actual implementation of access policies to succeed, the following will need to be done-

18.6.1.1 Ensure senior management support and commitment are in place for the new policy and for the consequent changes in the organisation's operations;

18.6.1.2 Ensure all personnel directly involved in administering access policies and procedures have been given formal responsibility for that work, through revisions to job descriptions if necessary;

18.6.1.3 Provide immediate and on-going education and training for all affected personnel, including producing and disseminating procedural manuals and guides to support implementation;

18.6.1.4 Meet regularly with all affected personnel to assess performance and address any concerns or questions; and

18.6.1.5 Monitor and evaluate the access programme regularly and make changes and improvements whenever necessary to achieve the best outcomes possible.

18.7 Any policy should be reviewed regularly, but it is especially important to review access policies when they involve electronic records or information. Since the technologies used to create records changes so rapidly, it is important to consider whether technological changes affect the nature or scope of the records covered by access policies or the ways in which the policies can be applied. Careful and regular review will ensure any organisation can then ensure it is always complying with both the letter and spirit of access legislation, ensuring the public's right to information is always protected.

19. TRAINING

19.1 Information officers should ensure that Records managers, if any, attend the Records Management Course to equip them with the necessary skills to enable them to perform their tasks.

19.2 After attending the course, the records managers should ensure that all staff members can read the filing system and be able to allocate file reference numbers to documentation. They should also ensure that all staff members are conversant with the proper registry procedures to enable them to support the Registry to function properly.

19.3 The records managers should ensure that all registry staff are equipped with the necessary skills to enable them to carry out their functions properly.

20. SECURITY OF ELECTRONIC RECORDS

20.1 A formal instrument that identifies the rights of access and the regime of restrictions applicable to records is a necessary tool to manage records in organisations of all sizes and jurisdictions. Reasonable security and access depend on both the nature and the size of the organisation, as well as the content and the value of the information requiring security. Public and private bodies must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

20.2 Electronic records must be protected from accidental or intentional damage or destruction and from any modification. Accordingly, organisation must, in accordance with section 19 of POPIA, secure the integrity and confidentiality of records in its possession or under its control by taking the following appropriate, reasonable technical and organisational measures to prevent loss of, damage to or unauthorised destruction of such records and unlawful access to the records-

20.2.1 identify all reasonably foreseeable internal and external risks to the records in its possession or under its control;

20.2.2 establish and maintain appropriate safeguards against the risks identified;

20.2.3 regularly verify that the safeguards are effectively implemented; and

20.2.4 ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

20.3 A public and private body must, in terms of a written contract between such body and any person in possession or control of the records of the body, ensure that such person establishes and maintains the security measures to ensure to the authenticity of stored information or prevent loss or damage to or unauthorised destruction of records.

20.4 **ISO/IEC 27001**[3] requires that management:

20.4.1 systematically examine the organisation's information security risks, taking account of the threats, vulnerabilities, and impacts.

20.4.2 design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and

20.4.3 adopt an overarching management process to ensure that the information security controls continue to meet the organisation's information security needs on an on-going basis.

20.5 Proof of compliance with the recommendation of ISO/IEC 27001 may provide helpful supporting evidence with the Regulator or in court, as it indicates that the organisation has exercised its duty of care and will assist the Regulator or the court in assessing the authenticity and integrity of information.

20.6 System administrators must set access privileges to protect records from unauthorized users. The tracking of records usage within records systems is a security measure for organisations. It ensures that only those users with appropriate permissions are performing authorized records tasks. The degree of control of access and recording of use depends on the nature of the business and the records it generates. For example, mandatory privacy protection measures in South Africa require that the use of records holding personal information be recorded and retained for such period as may be required or prescribed by law or a code of conduct.

20.7 The storage of records in electronic form necessitates the use of additional storage plans and strategies to prevent loss, damage or alteration of a record:

[3] **ISO/IEC 27001** is an international standard on how to manage information security, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It details requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) – the aim of which is to help organizations make the information assets they hold more secure. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

20.7.1 Backup systems are a method of copying electronic records to prevent loss of records through system failures. Such systems ought to include a regular backup schedule, multiple copies on a variety of media, dispersed storage locations for the backup copies, and provision for both routine access and urgent access to backup copies.

20.7.2 Maintenance processes may be needed to prevent physical damage to the media. Records may need to be copied to newer versions of the same media (or other new media) to prevent data erosion.

20.7.3 Hardware and software obsolescence may affect the readability of stored electronic records.

21. ELECTRONIC/DIGITAL SIGNATURES

21.1 The Regulator recommends the usage of an electronic or digital signature, as defined in section 1 of the Electronic Communications and Transactions Act, Act 25 of 2002.

21.2 Electronic signing is efficient and legally acceptable, offering several benefits, including:

21.2.1 Increased efficiency by getting documents signed off by various parties in different locations in minutes. Multiple parties can sign one document as part of a workflow process.

21.2.2 Trusted security because any changes made after the document is signed are detected immediately with complete transparency.

21.2.3 Savings on paper and printing costs, while providing an environmentally friendly alternative.

21.2.4 Most of the technologies are very easy to use with a clean user interface, even on portable devices.

22. OFFENCES

22.1 Destroying, damaging, or altering, concealing or falsifying a record is an offence, in terms of section 90 of PAIA.

22.2 Any person convicted of any of the above-mentioned offences shall be liable to a fine or to imprisonment for a period not exceeding two years.

23. CONCLUSION

23.1 Organisations should follow these guidelines in the management of their electronic records-

23.1.1 Maintain electronic records that are accessible, accurate, authentic, reliable, legible, and readable throughout their life cycle;

23.1.2 Document policies, assign responsibilities, and develop formal procedures for creating and maintaining electronic records;

23.1.3 Maintain confidentiality or restricted access to records maintained in electronic format;

23.1.4 Utilize information systems that accurately reproduce the records they create and maintain;

23.1.5 Design and maintain new information systems so they can provide an official record copy for those business functions completed or processed by the system;

23.1.6 Utilize information systems that can delete electronic records according to approved records retention schedules;

23.2 One way of proactively addressing electronic records management is to follow a standardized records management process, such as the one recommended in international standards. Accordingly, managers and others seeking to implement, operate and improve a management system for records are advised to use

ISO 15489, in conjunction with the **ISO 30300** and **ISO/IEC27001** series of International Standards.

23.3 The above-mentioned International Standards are adopted by the Regulator, for records management process under PAIA.

Issued by

INFORMATION REGULATOR
17 MARCH 2022

REFERENCE

a) Managing electronic records in governmental bodies: policy, principles and requirements- National Archives and Records Service of South Africa April 2006;

b) An Introduction to Digital Records Management- - ISACA (1 November 2010);

c) Electronic Records Management Guidelines Version 4, March 2004;

d) International Standards -ISO 15489, ISO 30300 and ISO/IEC27001;

d) Module 3: Managing the Creation, Use and Disposal of Electronic Records- International Records Management Trust, 2009.