ICT DATA MANAGEMENT POLICY

CGICT_ICT_001

Version 1.0 July 2021

Version Control and Approval			
Document Name	ICT DATA MANAGEMENT POLICY		
Document Number/Version	Version 1.0		
Status/Revision History			
Rev #	Revision Update	Revised By	Date
001	New Version 1	Mpumelelo Khumalo	28 July 2021
Approval			
Date Approved			
Date Last Amended	28 July 2021		
Date of Next Review	28 July 2023		
Related Policies and Legislation Frameworks	ICT Strategic Plan, Change Management Policy, Records Management Policy, Protection of Personal Information (POPI) Policy, IMC Information Management Policy (in compliance with National Archives Act), Minimum Information Security Standard (MISS), Electronic Communication and Transaction Act, Records Retention Policy (as prescribed by National Treasury), Protection of Personal Information (POPI) Policy		
Authored By			
Name	Mpumelelo Khumalo		
Position	Acting ICT Manager		
Signature		Date 30/05/2022	
Approved By			
Name	Sibongile Ngwenya		
Position	Corporate Services Executive		
Signature		Date 31/05/2022	
Approved By			
Name	Thamsanqa Mdontswa		
Position	Chief Executive Officer		
Signature		Date 31/05/2022	
Approved By			
Name	Portia Mushwana		
Position	Chairperson: ICT Steering Committee		
Signature	p mushwana	Date 10/6/2022	
Approved By			
Name	Chris Mudau		
Position	Chairperson of the Board		

Signature	Date

Table of Contents

1. Introduction

The Safety and Security Sector Education and Training Authority (SASSETA) has developed an ICT Strategic Plan or Master Systems Plan (MSP) that incorporates the Digital Transformation Strategy and outlines major ICT projects and initiatives to be undertaken by SASSETA in order to ensure that ICT supports and enables the mandate and business of the organisation.

The MSP or ICT Strategic Plan is intended to ensure that SASSETA manages Data as a critical asset that can provide a needed boost in enhancing the business operations and the achievement of strategic goals and objectives. In this regard, a Data Management Policy that is informed and based on the Data Management Strategy, will drive the unlocking of data and thereby improve the ICT consumer experience, streamline operations, provide the platform for quick responsiveness to services and innovate at speed.

SASSETA operates in a complex, data-oriented environment that requires those who are responsible for collecting, managing and disseminating data to do so in a systematic, planned and managed way. Data generated and held by the organisation are key assets that must be managed correctly in order to ensure that SASSETA functions efficiently and effectively. This policy outlines the data management framework that covers the roles that are responsible and accountable for data collection, storage, security, maintenance, dissemination and data quality.

This policy does not apply to:

- data from research projects or teaching activities, where these do not form part of the institutional data; or
- the collection of data for ad hoc or targeted/occasional usage.

This document provides a comprehensive data management framework which is consistent across SASSETA's major Lines of Business Systems. 'Data management' in this instance refers to the management of institutional data i.e., data which are required for the operation of the organisation.

2. Purpose

The Purpose of this ICT Data Management Policy is to establish and entrench a formal mechanism or data management process/system of managing ICT data within SASSETA with the main purpose of ensuring that data management responsibilities and principles apply to the management, security, and use of SASSETA's corporate assets and forms part of the organisations internal controls and corporate governance arrangements.

3. Scope

This framework applies to all SASSETA ICT related application systems that are hosted in-house,offsite, cloud and the digital data that is produced in the normal course of business from an operational and administrative perspective.

4. Definitions

TERM/ ACRONYM / ABBREVIATION	DEFINITION
Custodian	A member of the Senior Management Team (MANCO) responsible for the collection and dissemination of data in an information system. The Custodian is typically primarily responsible for the business function supported by a corresponding line of business system and the data used by it.
Data	A general term meaning facts, numbers, letters and symbols collected by various means and processed to produce information. Data may include personal or sensitive personal elements and needs to be managed in accordance with the relevant compliance and statutory obligations such as the SASSETA POPI Policy, ICT Security Policy (defines data/information protection and privacy), ICT Change Management Policy, HR Policy (regarding disciplinary procedure of disclosing POPI info), IMC Records Management Policy (in compliance with National Archives Act), Records Retention Policy (as prescribed by National Treasury).
Data Management	The management of institutional operational and administrative data i.e., data which are required for the operation of SASSETA.
Data Management Framework	The business processes and organisational structure in place to manage the SASSETA data resource.
Data Dictionary	A centralised repository of information about data such as meaning, relationships to other data, origin, usage and format.
Data Element	The fundamental data structure in a data processing system. Any unit of data defined for processing is a data element, e.g. Account Number, Name, Address, City and defined by size (in characters) and type (alphanumeric, numeric only, true/false, date etc.)
Data Set (Dataset)	A data set or (dataset) is a collection of data. Datasets can also consist of a collection of documents or files.
Data Quality	The accuracy, completeness, validity and currency of data.
Expert	Technical expert.
Information	Data that has been processed into a meaningful form.
Institutional Data	Data relevant to the operation of SASSETA (primarily data contained in Skills, Planning and Research, Learning Programmes, Education and Training Quality Assurance (ETQA), Human Resources (HR), Finance, Marketing and Communications, Call Centre, Information and Communications Technology (ICT), Facilities Management, Stakeholder Management and Governance Information systems.)

Line of Business System	A system that gathers, condenses, and filters data until it becomes information, then makes that information available on time and in a useful form for supporting decision-making at various levels of management within an organisation. Current examples include Indicium, Great Plains, SmartHR, MS Excel, Document Management System, Board Pack System, Business Intelligence System, Data Analytics System.
Steward	The person who has oversight of the use made of data and, as such, is the intermediary between users and experts.
Users	Staff who use operational and administrative data as part of their day-to-day work.

5. Policy Statement

The respective employees responsible for SASSETA's operations are also responsible for the institutional data that concerns the organisation. Maintaining the quality of this data is crucial to maximise the value of investments that SASSETA has made in data collection and maintenance, and so that internal and external decision-makers have confidence and trust in the information they rely on. SASSETA is committed to the following principles of data management and expects adherence to them.

6. Principles of Data Management

The following principles of data management outline best practices at a high level within SASSETA. Every Data Custodian (see below) must be aware of these, and adhere to them. This ensures contributions to data quality are being made at all levels within the organisation.

These principles must guide all data management procedures.

1. The SASSETA organisation, rather than any individual or business unit, owns all data.
2. Every data source must have a defined Custodian in a business leadership role, who has overall responsibility for the accuracy, integrity, and security of those data.
3. Wherever possible, data must be simple to enter, be clearly defined and accurately document their subject. They must also be in a useful, usable form for both input and output.
4. Data should only be collected for a specific and documented purpose.
5. Data must be readily available to those with a legitimate business need.
6. Data capture, validation, and processing should be automated wherever possible.
7. Data must be entered only once.
8. Processes that update a given data element must be standard across the information system.
9. Data must be recorded as accurately and completely as possible, by the most informed source, as close as possible to their point of creation, and in an electronic form at the earliest opportunity.
10. Data should be recorded and managed over time in an auditable and traceable

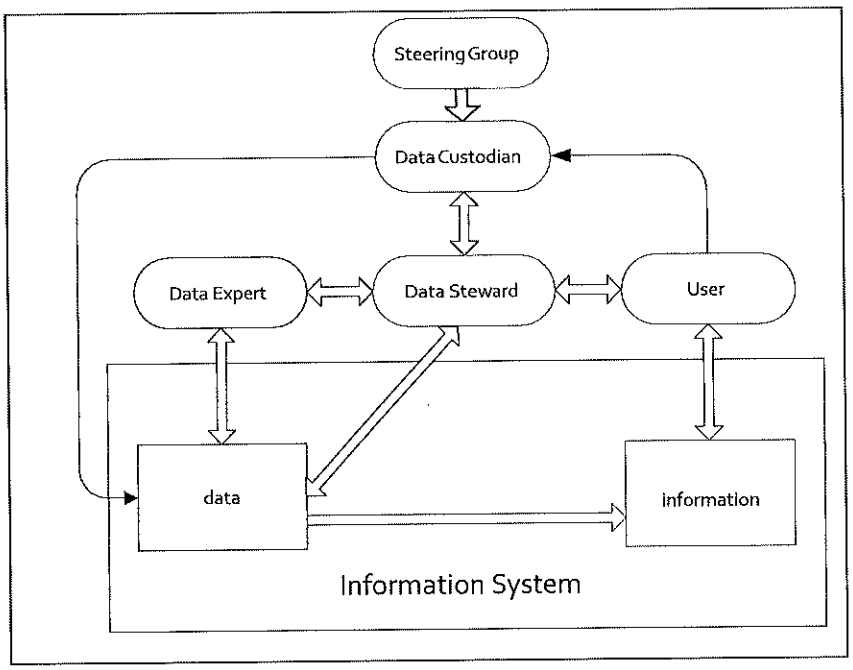
manner.

11. The cost of data collection must be minimised.
12. Data must be protected from unauthorised access and modification.
13. Data must not be duplicated unless duplication is essential and has the approval of the relevant Data Steward. In such cases, one source must be clearly identified as the master; there must be a robust process to keep the copies in step; and copies must not be modified (i.e., ensuring that the data in the source system is the same as that in other databases).
14. Data structures must be under strict change control, so that the various business and system implications of any change can be properly managed.
15. Whenever possible, international, national, or industry standards for common data models must be adopted. When this is not possible, organisational standards must be developed, documented and implemented.
16. Data should be defined consistently across SASSETA.
17. Users must accurately present the data in any use that is made of them.
18. Schemas that describe the data must be developed and maintained for as long as the data that they describe are in use, and these must be maintained separately to the systems that manage the data.

7. Data Management Roles and Accountabilities

In order to ensure that data are consistent, correct, and available to those with legitimate requirements, the establishment of the following data management roles for each major Line of Business System is necessary. This establishes a data management framework which is consistent across SASSETA.

Figure 1: Data Management Framework:



The Information Governance Group is charged by the Chief Executive Officer and Corporate Services Executive with acting as a governance body (steering group) in relation to the SASSETA's information environment.

The **Data Custodian**, holding delegated authority from the Chief Executive Officer and Corporate Services Executive, is responsible for the business function the Line of Business System performs and all the data associated with it.

The **Steward** has oversight of the data use/s and is thus the intermediary between experts and users.

The **Data Expert** is primarily concerned with data and the technical aspects surrounding data management.

The **User** works with operational and administrative data and where necessary, transforms this into information.

Information Governance Group

The purpose of the Information Governance Group is to ensure that the SASSETA Information Strategy and related policies are given effect; and that the organisation develops the frameworks and environments from which benefits and efficiencies can be realised, while mitigating risks and issues associated with managing significant information holdings.

With respect to data management, the purpose of the Information Governance Group is to:

- oversee the Data Management Framework (see above), and ensure its alignment with other SASSETA information management initiatives and strategies;
- ensure systems are compliant with SASSETA's policies and external mandates;
- oversee and report on risks to information assets (including data);
- advise key stakeholders on data management risks and issues;
- oversee the implementation and compliance with this policy; and
- ensure proper and effective coordination of the operation and outputs of all SASSETA's Line of Business Systems, and adjudicate on disputes that may arise from time to time.

Data Custodian

The Data Custodian is a Senior Management Team (MANCO) member with delegated responsibility from the Chief Executive Officer and Corporate Services Executive for the collection, dissemination and security of data in a major information system.

The establishment of the Data Custodian role is based on two key concepts:

1. Data are critical to SASSETA and must be shared across the organisation.
2. Data assets must be coordinated across SASSETA at the highest level to ensure maximum return on investment.

The overriding philosophy of data custodianship should be one of a trustee acting in partnership with all participants. Custodianship reinforces the concept of one individual being ultimately responsible and accountable for the information that others might use. The Data Custodian provides guidance, decision-making and leadership for the Data Stewards (below), so that SASSETA-wide information needs are met. Data Custodians are senior members of staff within SASSETA. They are not expected to carry out the necessary work themselves; their role is to ensure that visibility and responsibility for their data is

articulated from a senior level to ensure progression towards a common goal of high quality and clearly defined data. Actions should be guided by the principles of data management outlined above.

Responsible for:

- understanding legislation and SASSETA policies surrounding data e.g., privacy, protected disclosures, communications, official information, records management, as well as consequences of misuse of data, the legal and administrative consequences of maintaining and disseminating data within their custody;
- corporate use of data, in both uploading and downloading data;
- data quality;
- security;
- customised business interpretations (and negotiates with Data Steward for delivery of reporting functions); and
- change management – will provide advance notice of proposed business changes and corresponding impacts on data structures and will negotiate resources necessary to implement the change (i.e., the Data Custodian is the one who decides the necessity for change rather than the Data Steward or the Data Experts).

Data Steward

The Data Steward coordinates Data Experts (outlined below) and business users from across SASSETA. By using their knowledge and collective views about the data and issues faced by the user community; issues can be addressed in a SASSETA-wide context. The Data Steward must understand the larger business context in which the data will be used and should be able to relate SASSETA's user needs to specific technical capabilities and requirements.

Responsible for:

- ensuring data in each system are accurate, complete, valid and up to date;
- working with Data Experts to define appropriate nomenclature, data definitions, and documenting these;
- working with system designers, data experts and technical experts on applying business rules governing data migration and data retention and disposal and permissions/access management; data quality monitoring; and
- maintenance of data quality and security.

Tasks within relevant Operational and Administrative Systems:

- establish procedures governing data elements;
- establish access authorisation procedures;
- determine and evaluate the most reliable source of data;
- make data dictionary understandable to users;
- ensure that only needed versions of each element exist;
- assign responsibilities for data integrity;
- resolve conflicts involving shareable data;
- consult with users on use of electronic data;
- analyse and enhance data quality;
- maintain direct expertise in the data set;
- control data entry into a system;
- maintain data integrity;
- develop and maintain standard entity definitions;
- develop standard attribute definitions;
- document data definitions, calculations, summarisations, etc.;
- provide customised reporting;
- establish data security specification; and

- apply data retention criteria.

Data Experts

These are staff with detailed technical knowledge and experience in their respective data processing and application areas. They understand the technical framework supporting SASSETA's data processing and management activities.

Data Experts cannot act as Data Stewards or Data Custodians because those positions are responsible for SASSETA's operations and are also responsible for the institutional data concerning these operations.

Responsible for:

- delivering data and providing the infrastructure, security and data framework for delivering quality data in a timely fashion to SASSETA's stakeholders and clients;
- carrying out data quality analyses;
- ensuring technical security; and
- deploying the requisite technology.

Users

Everybody who uses data throughout the organisation must understand their role in data quality and be able to provide feedback that will help prevent bad data habits spreading throughout SASSETA. It is important that users are aware of the many uses of data in order to understand how crucial sensitive, confidential and high-quality data are to the operations of SASSETA.

Security

SASSETA acknowledges an obligation to ensure appropriate security for all institutional data in its domain of ownership and control.
Application level security at SASSETA is generally well set up and managed. This policy ensures consistent application of the same security across all information systems within the organisation. Security must be directly related to the category in which data are classified. These categories being: public data, general administrative data, operational data, protected data, and restricted data.
There are two aspects surrounding the security of operational and administrative data:
1. **Data security** – refers to user access, and the amount of access each user is allowed. Data security is administered by Data Custodians (or by delegation to Data Stewards). The technical security framework is the responsibility of Data Experts.
2. **Physical security** – Data Users throughout SASSETA must understand that certain information is privileged and should be kept secure. Physical security is important to ensure unauthorised access does not occur. Physical security is the responsibility of all staff.

8. Data Management

To ensure compliance to the POPIA, SASSETA developed the Protection of Personal Information (POPI) policy to outline its compliance approach, as a skills development Sector Education and Training Authority (SETA) in administering and enforcing aspects of the relevant promulgated laws, regulations, directives, prescripts, and standards of good practice. The policy also provides the key elements of SASSETA's compliance approach and the adherence /compliance to the policy, the associated risks and staff and stakeholder awareness relating to the protection of personal information and data.

9. Framework Implementation

The ICT Business Unit and Corporate Services are accountable and shall also be responsible for its future amendments or reviews.

The Chief Executive Officer (CEO) is accountable for the overall framework implementation and reserves the right to intervene and take necessary steps when the framework is not adhered to. The accountability may be delegated to the Executive Manager: Corporate Services or any other Manager deemed fit for the function. Business Unit Heads, in consultation with ICT, are responsible for the framework implementation in their respective divisions.

9. Non-Compliance to the Framework

Non-compliance with the application of the framework would be subject to disciplinary procedures being invoked in terms of the SASSETA Disciplinary Policy, where disciplinary action could result in consequences due to non-compliance.

10. Framework Validity

This framework will be effective from the date of approval. In an event of any doubt about the authenticity of a framework document, the document signed by the Chief Executive Officer (CEO) shall be considered as the only document with validity, authority and a force of law.

This framework shall be reviewed every two years or if there are major changes in the ICT legislative environment.