ICT Change Management Policy

CGICT_ICT_002

Version 1.3 August 2021

Version Control and Approval			
Document Name		ICT Change Management Policy	
Document Number/Version		1.3	
Status/Revision History			
Rev #	**Revision Update**	**Revised By**	**Date**
1.0	**New**	Author: William Nkuna	April 2017
1.1	Revision	Author: William Nkuna	September 2019
1.2	Revision	Author: William Nkuna	November 2019
1.3	Revision	Author: Mpumelelo Khumalo	August 2021
Approval			
Date Approved			
Date Last Amended		August 2021	
Date of Next Review		2023/24	
Related Policies			
Authored By			
Name		Mr. Mpumelelo Khumalo	
Position		Acting ICT Manager	
Signature			Date: 31/08/2022
Reviewed and Recommended by			
Name		Ms. Sibongile Ngwenya	
Position		Executive Manager: Corporate Services	
Signature			Date: 30/03/2022
Name		Mr. Thamsanqa Mdontswa	
Position		Chief Executive Officer	
Signature			Date: 30/03/2022
Approved By			
Name		Ms. Portia Mushwana	
Position		Chairperson: ICT Steering Committee	
Signature			Date: 30/03/2022
Approved By			
Name		Mr Chris Mudau	
Position		Chairperson: Board and Accounting Authority	
Signature			Date: 30/03/2022

Table of Contents

1 INTRODUCTION 4

1.1 PURPOSE 4

1.2 SCOPE 5

1.3 DEFINITIONS AND TERMS 5

2 POLICY STATEMENT 6

3 POLICY OBJECTIVES 6

4 POLICY 6

4.1 GUIDELINES AND BUSINESS RULES 6

4.2 CHANGE PROCESS 7

4.3 EMERGENCY CHANGES 9

5 ROLES AND RESPONSIBILITIES 9

6 LEGISLATION 11

7 POLICY IMPLEMENTATION 11

8 NON COMPLIANCE TO THE POLICY 11

9 POLICY VALIDITY 11

1 Introduction

Operational change management brings discipline and quality control to ICT and related Information Systems. Attention to governance and formal policies and procedures will ensure its success. Adopting formalised governance and policies for operational change management delivers a more disciplined, efficient and effective infrastructure and a stable systems environment. This formalisation requires communication; the documentation of important process workflows and personnel roles; and the alignment of automation tools, where appropriate.

The Safety and Security Sector Education and Training Authority SASSETA management has recognised the importance of change management and control and the associated risks with ineffective change management. The Change Management Policy had been formally documented to address the opportunities and associated risks.

The Safety and Security Sector Education and Training Authority (SASSETA) ICT Change Management Policy is developed to be uniform and provide guidelines regarding the Change Management process within the ICT unit and encompassing operating systems, business systems and applications. The Change Management policy has been developed to assist SASSETA, managers and staff to effectively manage and participate in the change management processes at SASSETA. The following stakeholders were consulted in the development of the policy:

- SASSETA current ICT Process Owners;
- SASSETA Strategic ICT Service providers;
- SASSETA ICT Steering Committee; and
- SASSETA Management

1.1 Purpose

The Purpose of this Policy is to guide ICT change relating to operations within SASSETA. Change Management is a method by which programmatic and system changes on a system are formally defined, documented, evaluated and approved. The process entails completing a variety of control procedures to ensure that continuous improvement and impact of key organisational deliverables are achieved in a consistent, stable, controlled and optimal manner.

Furthermore, this policy's purpose is to establish management direction and high-level objectives for change management and control. This policy will ensure the implementation of change management and control strategies and procedures to mitigate associated risks such as:

- Implementation of unauthorised changes;
- Information being corrupted and/or destroyed;
- Computer performance being disrupted and/or degraded;
- Productivity losses being incurred; and
- Exposure to operational and reputational risk.

Furthermore, the implementation of the policy will ensure that every change identified is formally:

- Communicated
- Documented
- Analysed
- Reviewed
- Tested
- Approved
- Implemented

1.2 Scope

This policy applies to all parties operating within SASSETA's network environment or utilising Information Resources. It covers data networks, LAN servers, Operating systems, Application systems and personal computers (stand-alone or network-enabled) located at company offices and company production related locations, where these systems are under the jurisdiction and/or ownership of SASSETA, and any personal computers, laptops, mobile devices and or servers authorised to access the SASSETA's data networks.

NB: No employee is exempt from this policy

1.3 Definitions and Terms

Term/Acronym	Definition
A Service Request	Is defined as a user-initiated request for the provision of a new service or an enhancement that is not classified as a change to an existing application or supporting infrastructure.
Backup	The activity of creating a copy of a file(s) and/or folders which is stored separately from the original data, to preserve in the event of accidental data loss, disasters or due to data that is inaccessible.
Change	Any implementation of new functionality, any interruption of service, any repair of existing functionality and any removal of existing functionality.
Change Management	The process of controlling modifications to hardware, software, firmware and documentation to ensure that information resources are protected against improper modification before, during, and after system implementation.
Change Review	The process followed to determine if changes made to ICT infrastructure, systems and devices are in accordance to the approved requirements.
Change Request form	A formal request document stating the required change in the ICT environment required which needs to be completed by a requester.
Requester	The name of the person requesting the change.
RFCs	Requests for Change.
User	Any person defined as an employee, sub-contractor, vendor support staff or temporary staff who has permission granted by the SASSETA management to access the software application or SASSETA networks.
Information Resources	All data, information as well as the hardware, software, personnel and processes involved with the storage, processing and output of such

	information. This includes data networks, servers, PC's, storage media, printers photo copiers, fax machines, supporting equipment, fallback equipment and back-up media.
Audit Trail	A record or series of records which allows the processing carried out by a computer system to be accurately identified, as well as verifying the authenticity of such amendments.

2 Policy Statement

The SASSETA Change Management policy ensures that standardised methods and procedures are used to alter the environment to minimise the risk for negative impact on change.

3 Policy Objectives

This policy aims to address the processes to be followed when there are Requests for Change (RFCs) that involve the following aspects of the entity's infrastructure:

- Hardware and Communications Equipment;
- Application Software and Software Database;
- System Software;
- Server room environment;
- Infrastructure Management; and
- Environment Systems.

4 Policy

4.1 Guidelines and business rules

a) Changes to information resources shall be managed and executed according to a formal change control process.
b) The control process will ensure that changes proposed are documented, reviewed, authorised, tested, implemented, and released in a controlled manner; and that the status of each proposed change is monitored.
c) All changes to the SASSETA information technology environment must be in accordance with the Change Management Policy and must adhere to the Change Management Procedures and Guidelines.
d) The change request forms are available on the ICT share drive and all requesters are required to complete the "Change Request form".
e) All change requests must be approved by the line managers and system owner prior to submission to the ICT Manager.
f) All employees affected by the possible change must be informed prior to the approved change.
g) Backups must be performed prior to the commencement of system changes.
h) All changes must be tested prior to being submitted to the SASSETA environment.
i) The migration from test environment to the live or production business environment must be documented and approved.

j) All changes must be submitted to the ICT Manager and Line Management for review to ensure all changes made are in accordance with the change request.

k) The following types of changes that can be made will be classified as follows:
   a. Standard change: An "ITIL" standard change is a change to a service or infrastructure for which the approach is pre-authorised by change management that has an accepted and established procedure to provide a specific change requirement.
   b. Emergency change: An "ITIL" emergency change is the highest priority change that can be defined in an organisation. Emergency changes are defined as changes that need to be evaluated, assessed and either rejected or approved in a short space of time.
   c. Urgent changes; changes that are required quickly due to a pressing need such as a legal requirement or a business need but are not related to restoring service.

4.2 Change Process

The normal change process steps include:

- The submission of change requests
- The review and logging of change requests
- The determination of the feasibility of change requests
- The approval of change requests
- The implementation and closure of change requests.

Process Procedure	Process Description
Create and record RFC	The project team, line Managers, Super Users, ICT Manager and Developers and other relevant stakeholders will raise the RFC. Each RFC will detail a single change with sufficient detail to ensure the project/operational team understand the requirements. The RFC form summarises the changes. Description, Justification, Benefits, Costs, Impacts, Any supporting documentation, Approvals must be included in the RFC.
Review, filter and prioritise	The ICT Manager will review, filter and prioritise all requests. The ICT Manager will determine whether or not additional information is required to assess the full impact of the change to the project time, scope and cost. The decision will be based on factors such as: • Number of change options presented • Feasibility and benefits of the change • Complexity and/or difficulty of the change options requested • Scale and scope of the change solutions proposed.
Assess and Evaluate	The ICT Manager and Senior Management then consider the Change Request form and any supporting documentation for approval. Review and final approval. Assessment will take place using the 7Rs – Raised, Reason, Return, Risks, Resources, Responsible and Relationships.
/Reject	ICT Manager and senior Management may: • Agree authority of change

	• Reject the Change • Request for more information related to the change • Approve the change as requested • Approve the change subject to specified conditions This will include a review against business risk, financial implications and scope of change. There will be a "right to appeal" and the Unit Manager can appeal to the CEO when a change is rejected.
• Plan update • Co-ordinate Implementation • Review and close	**If the change is approved, the following will occur:** • Approve the change request by signing the change control form • An implementation date of the change will be identified • A test of the change will be done • The change requester will approve the change implementation • The change will be implemented if successful • The implementation of the change will be reviewed and deemed successful or corrective actions taken • The conclusion of the change implementation will be communicated to all relevant parties
	Approved changes, documented Project Plan and work packages updated.
	ICT Team co-ordinates changes. Recovery procedures prepared (to return to known state if necessary). Changes tested. Implementation schedule agreed to ensure least impact on live services.
	ICT Team performs the post implementation review. Changes checked against objectives, related incidents, problems dealt with and closed, and lessons learnt.
Rollback plan	The following steps will be required to restore the system to its original state. The plan must be detailed enough for an appropriately skilled technician to understand and execute the rollback successfully. **Approving a Change Request** Change Owner ensures that the Change Request Form, including Implementation, Test, Rollback and Contingency plans, and notification list is complete and that scheduling of the change is appropriate. An individual requesting a change must make a request in writing and send it to the Help Desk by e-mail. Where expertise allows, the requestor is expected to draft and attach a Change Request Form including the following: • Implementation Plan, Test Plan, Rollback or Contingency Plan

4.3 Emergency Changes

The ICT Manager in conjunction and agreement with the line function Manager have the authority to make emergency decisions when a major problem arises and it becomes necessary to implement an RFC before the Senior Management is able to review the request.

Once the change has been implemented, the process to formally approve the change should be retrospectively followed and implemented.

5 Roles and Responsibilities

Role	Functional Responsibilities
Members of the ICT Steering Committee	• Members of the ICT Steering Committee shall ensure that the ICT Change Management Policy has been implemented.
Information Security roles and responsibilities	• Establish and revise the information security strategy, policy and standards for change management and control with input from interest groups and stakeholders; • Facilitate and co-ordinate the necessary counter measures to change management and control initiatives and evaluate such policies and standards; • Establish the security requirements for change management and control directives and approval of the change management and control standards and change control/ version control products; • Co-ordinate the overall communication and awareness strategy for change management; • Acts as the management champion for change management and control; • Provide technical input to the service requirements and co-ordinate affected changes to SLA's where applicable. • Establish and co-ordinate appropriate interest group forums to represent, provide feedback, implement and monitor change management and control initiatives; and • Co-ordinate the implementation of new or additional security controls for change management.
ICT Manager	• Implement, maintain and update the change management and control strategy, baselines, standards, policies and procedures with input from all stakeholders; • Approve and authorise change management and control measures on behalf of the organisation. • Ensure that all application owners are aware of the applicable policies, standards, procedures and guidelines for change management and control;

	• Ensure that policy, standards and procedural changes are communicated to applicable owners and management forums; • Appoint the necessary representation to the interest groups and other forums created by each company for Information Security Management relating to change management and control; • Establish and revise the information security strategy, policy and standards for change management and control; • Report and evaluate changes to change management and control policies and standards; • Co-ordinate the overall communication and awareness strategy for change management and control; • Co-ordinate the implementation of new or additional security controls for change management and control • Review the effectiveness of change management and control strategy and implement remedial controls where deficiencies are identified; • Provide regular updates on change management and control initiatives and the suitable application; • Evaluate and recommend changes to change management/ version control solutions; and • Establish and implement the necessary standards and procedures that conform to the Information Security policy; • Responsible for approving, authorising, monitoring and enforcing change management initiatives and related security controls within the organisation; • Ensure that all solution owners are aware of policies, standards, procedures and guidelines for change management and control. • Ensure the compliance of this policy and report deviations to the ICT Manager and Executive: Corporate Services.
ICT Service Provider	• Shall comply with all change management and control statements of this policy.
Application	• Shall comply with all information security policies, standards and procedures for change management and control; and • Report all deviations.

6 Legislation

The South African laws and policy frameworks that underpin this policy include the following:

- Promotion of Access to information Act, 200 (Act 2 of 2000)
- Protection of Information Act, 1982 (Act 84 of 1982)
- Protection of Personal Information Act, 2013 (Act 4 of 2013)

The following policies and procedures are related to the Change Management Policy:

- Information Security Policy
- Acceptable Use Policy
- Patch Management Policy

7 Policy Implementation

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

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

8 Non Compliance to the Policy

The policy should be used in conjunction with the SASSETA Disciplinary Policy, where disciplinary action could be a consequence due to non-compliance.

9 Policy Validity

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