INFORMATION TECHNOLOGY CHANGE MANAGEMENT POLICY

PURPOSE

The purpose of this Information Technology Change Management Policy is to establish the framework and guidelines for managing changes to information technology (IT) systems, applications, and infrastructure. It aims to ensure that changes are implemented in a controlled, efficient and transparent manner, with minimal disruption to services and operations.

OBJECTIVE

This policy applies to all IT change requests, submitted by employees, contractors, or third-party vendors within the organisation and changes deemed necessary and worthwhile by IT Services. It covers, but is not limited to, changes to hardware, software, applications, databases, networks, CCTV, mobile devices, security, and other IT components.

POLICY

This policy applies to all employees, contractors, third-party vendors and Elected Members.

APPLICATION – CHANGE REQUEST PROCESS

All IT change requests must be made through a formal change request process. This process should include the following steps:

i. Request Initiation: The requester must submit a formal change request, providing a detailed description of the proposed change and the reason for the change. The request itself must be in writing on the designated IT Change Request Form and sent to the Executive Manager Corporate Services but must have a minimum of manager level of approval.
ii. Change Review: The change requested should be reviewed by the requester's Executive Manager to determine its feasibility, impact and potential risks.
iii. Change Approval: Once the review is complete, the Executive Manager Corporate Services will approve or deny the change request based on its potential impact on IT systems, processes, financial considerations, and operations.
iv. Change Implementation: The Executive Manager Corporate Services will execute the change internally or via approved external IT Services.
v. Monitor and Review: The Executive Manager Corporate Services will regularly review the change requirements to ensure relevance.

CHANGE MANAGEMENT ROLES AND RESPONSIBILITIES

All employees, contractors, and third-party vendors involved in IT change requests should understand their roles and responsibilities in the change management process. The key roles include:

a. Change Requester: The individual who initiates the change request.
b. Change Manager: The designated individual responsible for viewing, approving and managing the changes.
c. Change implementer: The individual responsible for implementing approved changes.

d. Change Monitor: The individual responsible for monitoring changes and ensuring that they are functioning as expected.

CHANGE COMMUNICATION AND DOCUMENTATION

All changes should be communicated to relevant stakeholders and documented in a centralised change management system. The documentation should include details such as the reason for the change, the impact on IT systems and processes, the implementation schedule, a financial analysis and the results of testing and verification.

CHANGE CONTROL AND RISK MANAGEMENT

All IT changes must be controlled and managed to minimise the risk of negative impact on IT systems, processes, and operations. Risk assessment should be performed before making any change, and appropriate controls should be in place to mitigate any potential risks.

CHANGE MANAGEMENT REVIEW

The change management process should be reviewed periodically to ensure that it remains effective and efficient. The review should include an assessment of the policy's effectiveness, recommendations for improvements, and feedback from stakeholders.

Annexure A –

STATUTORY ENVIRONMENT

Local Government Act 1995

Record of Policy Review						
Version	Author	Council Adoption	Resolution	Reason for Review	Next Review Date	CEO Signature
01	Tricia Brown	27/02/2025	111 - 24/25	New Policy	Feb 27	

ANNEXURE A – IT CHANGE REQUEST FORM

IT CHANGE REQUEST

DATE: _____

REQUESTING OFFICER: _____

REASON FOR REQUEST: _____

Actions and Reasoning:

CHANGE IMPLEMENTER USE ONLY

RISKS ASSESSED: Y ☐ N ☐

EMCS CHECKED: _____ SIGNATURE: _____

REJECTED: ☐ ACCEPTED ☐

REASON REJECTED: _____

CHANGE IMPLEMENTATION DATE: _____

	RISK PROFILE	RISK ASSESSED
1	Operational Risk: 1. Disruption to Service 2. Resource Strain 3. Increased Workload	
2	Organisational Risks: 1. Resistance to Change 2. Cultural Impact 3. Leadership or Governance Challenges	
3	Technological Risks: 1. System Failures or Downtime: 2. Data Security & Privacy Concerns 3. Integration Challenges	
4	Financial Risks: 1. Budget Overruns 2. Funding Shortfalls 3. Return on Investment	
5	Legal and Compliance Risks 1. Non-Compliance with Regulations 2. Contractual Risks 3. Litigation Risk	
6	Human Resources Risks 1. Employee Morale 2. Talent Retention 3. Training & Skills Gap	
7	Strategic & Long-Term Risks 1. Misalignment with Strategic Goals 2. Long Term Sustainability 3. Scope Creep	
	CHANGE MANAGER	**SIGNATURE**

1. Operational Risks

- Disruption to Services: Changes may cause interruptions to critical services or processes, affecting the delivery of government services to the public.
- Resource Strain: Insufficient resources (staff, budget, equipment) may result in delays or ineffective implementation of the change.
- Overload on Staff: Increased workload on employees due to the change can lead to burnout, reduced productivity, and decreased morale.

2. Organizational Risks

- Resistance to Change: Employees and other stakeholders may resist the change due to fear of the unknown, perceived loss of job security, or scepticism about the effectiveness of the change.
- Cultural Impact: Changes may conflict with the existing organizational culture, leading to disengagement, miscommunication, and internal conflict.
- Leadership or Governance Challenges: Lack of clear leadership or governance structures during the change process can result in confusion, poor decision-making, or inconsistent implementation.

3. Technological Risks

- System Failures or Downtime: If the change involves technological updates or new systems, there is a risk of system malfunctions, incompatibility, or downtime that disrupt operations.
- Data Security and Privacy Concerns: Introducing new technologies or systems may expose sensitive data to security risks, increasing the potential for data breaches, cyberattacks, or non-compliance with privacy regulations.
- Integration Challenges: New technologies or systems may not integrate well with existing infrastructure, leading to inefficiencies or additional costs for troubleshooting.

4. Financial Risks

- Budget Overruns: The change may exceed the initially allocated budget due to unforeseen expenses, poor planning, or scope creep.
- Funding Shortfalls: Insufficient funding to support the change process, including training, new technologies, or resource allocation, could halt or delay the initiative.
- Return on Investment (ROI) Uncertainty: There may be a risk that the anticipated benefits of the change, such as cost savings or improved efficiency, do not materialize as expected.

5. Legal and Compliance Risks

- Non-Compliance with Regulations: Changes, especially those involving new technologies or processes, could lead to non-compliance with local, state, or federal laws, regulations, or standards.
- Contractual Risks: If the change involves contracts with third-party vendors or service providers, there may be risks related to breach of contract, failure to meet agreed terms, or disputes over contract fulfillment.
- Litigation Risk: Changes that negatively affect employees or the public could result in lawsuits, complaints, or legal challenges, particularly if due process or consultation was not followed

6. Human Resources Risks

- Employee Morale: Employees may feel demotivated or uncertain about their future due to changes in policies, structure, or job roles, leading to lower morale or productivity.
- Talent Retention: Significant changes, especially those involving restructuring, can lead to a loss of experienced staff or difficulty attracting new talent.
- Training and Skill Gaps: If employees are not adequately trained for new roles, systems, or processes, it could result in skill gaps, mistakes, and inefficiencies.

7. Strategic and Long-term Risks

- Misalignment with Strategic Goals: The change may not align with the broader strategic goals or priorities of the local government, leading to inefficiency or diversion of resources from more critical initiatives.

- Long-term Sustainability: While a change might bring short-term benefits, there is a risk that the long-term sustainability of the change is not adequately considered (e.g., through continued funding, infrastructure, or human resources).

- Scope Creep: Over time, the scope of the change initiative might expand beyond the original objectives, leading to a loss of focus, inefficiencies, or unanticipated consequences.