COUNCIL POLICY			
CHANGE MANAGEMENT POLICY	Policy No:		
	Adopted by Council:		21 June 2018
	Next review date:		June 2019

Senior Manager:	Director Corporate and Community Services
Responsible Officer:	Director Corporate and Community Services
Functional Area:	Corporate Services / Information Technology

Introduction & Background	Council operates in a dynamic and evolving landscape where information needs and requirements are fluid. To keep up with this Council will from time to time require changes to its Information and Communication Technology (ICT) platforms to be made. For this change to be effective, Council needs to undertake and manage it in a co-ordinated manner.
Purpose & Objectives	This policy provides a high level framework to provide a management process to be followed for all ICT service changes, concentrating on the management, approval and communication of change. This policy does not apply to regular system maintenance functions.
Definitions	ICT system:- any Information or Communications Technology system that Council employs to manage, collect and store information. Change:- Any alteration to the current running configuration of an ICT system. Change Manager:- A Council Officer responsible for managing the change process on behalf of Council.

Policy Details

1.	Overview
	Council employs a number of ICT systems to manage its business. To keep abreast of changes to business Council will periodically need to make changes to these systems. There are four basic steps in the change process:

1. Initiating Change
2. Change Approval
3. Change Implementation

		4. Accepting Change
2.	Initiating Change	
	A change is initiated when Council becomes aware that the current systems will no longer perform to the level required. This may result from a number of sources, including: • Legislative or regulatory change • Obsolescence of Council's existing systems • Supplier initiated change (i.e support requirements, software patches, etc) • Security threats • Other Council initiated reasons At the initiation stage the change required will be documented clearly showing: • Requirement for the Change • System(s) affected • Risk of change (including risk of not changing) and level of urgency • Identified affected stakeholders • Testing plan including success or failure thresholds • Resources required to implement change including timeline • Costs involved with the change	
3.	Change Approval	
	Once documented the change shall be presented to management for approval. Depending upon the level of change this may be an individual manager, director, or the Chief Executive Officer. (See Appendix A for more information) If the change is approved then a Change Manager shall be appointed to manage the change implementation on behalf of Council.	
4.	Change Implementation	
	Once the change approval has been granted the Change Manager shall implement the change. It is the responsibility of the Change Manager to ensure that all pre-implementation dependencies and requirements (i.e that a backup is taken, or contractors are arranged, etc) are in place before implementation is undertaken. The Change Manager has delegated authority from Senior Management to make whatever operational actions are required to implement the change within the scope of that change process.	

	More complex implementations may require regular implementation or milestone reporting to management – this will be at the discretion of management when approving the change project. It is the responsibility of the Change Manager to implement a comprehensive testing regimen on any change implemented. The implementation phase of the change project must not be completed until testing has been complete. If testing highlights a problem with the implementation of the change then the Change Manager must immediately report this to management. Management in conjunction with the Change Manager will then investigate and review the problems with a view to producing a mitigation strategy.	
5.	Accepting Change	
	Upon practical completion of the project the Change Manager must measure the success and failure of the change implementation and provide a project completion report to management. Management will assess the project completion report before accepting it and closing the change project. If management assesses that the project should be closed, then a remedial action plan shall be produced and returned to the Change Manager for implementation.	

Policy Adopted:	Ordinary Meeting 21/06/18	Minute Book Page 38111	RecFind 18/002251
Policy Reviewed:	Ordinary Meeting __/__/19	Minute Book Page _____	RecFind 19/00_____

APPENDIX A

Levels of Change and Risk

Change may be categorised into four broad categories:

1. Routine Change – Any change that is minor and routine in nature, such as installing a routine software patch or minor update. A routine change is one which exhibits low risk and involves minimal system downtime. A relevant manager may authorise this level of change. Documentation may be of a minimal nature, such as emails and testing logs.

2. Normal Change – Any change which involves a low or medium risk which is not of routine or incidental nature, but nonetheless is still a known and planned change. Examples of normal change are implantation of major software, upgrades for example, new versions of Microsoft Excel or Word, Corporate Software updates, etc. These are changes which may involve minor system downtime. Normal Change must be authorised by a Director or the CEO. Documentation must involve formal request for change and authorisations and detailed testing logs must be produced and maintained.

3. Major Change – Any change which requires the implementation of a new ICT system software and/or hardware. This may be replacement of an existing system or a new additional system. Major change normally carries inherent high risk activities to Council. Authorisation of major change must come from the CEO or Council if a public tender is involved. Comprehensive documentation is required, including detailed planning documentation and regular implantation briefings and reports. A detailed testing regimen must be undertaken and documented.

4. Emergency Change – An emergency change is one which must be implemented as soon as possible. These may result from major incident or security issues, or from a sudden regulatory change. An emergency change generally carries high risk and must be authorised by a director or the CEO. Detailed implementation and testing documentation must be maintained.

Risk is a combination of urgency and failure consequence. Both urgency and failure consequence may be categorised in three major categories:

Risk	Urgency
Low	Minor impact on day to day activity of Council
Medium	Moderate effect – change should occur to achieve best practice
High	Major change which must be undertaken to maintain business operations

Risk	Fail Consequence
Low	Minimal impact, insignificant financial and time loss, no reputational consequence
Medium	Moderate time loss (<5 days), financial loss (<$50,000), localised reputational damage
High	Significant time loss (>5 days), significant financial loss (>$50,000), national reputational loss, failure to comply with legislative or legal requirements.