Credit Union		IT Credit Union Information Systems Change Management Policy			
Policy No: CU-P15	**Version:** 2.0	**Issue Date:** June 2023		Page 1 of 6	
Ver.	**Amendment Description / Review information**	**Created / Revised / Modified By**	**Date**	**Approved by Board**	**Review Date**

Signed: Position: Date:

_____ Chairman

_____ Secretary

Table of Contents

1. PURPOSE, SCOPE AND USERS 3
2. POLICY 3
2.1 SCOPE AND GOALS OF CHANGE MANAGEMENT PROCESS 3
2.2 UNAUTHORISED CHANGES 3
2.3 PROCESS GUIDELINES 4
2.3.1 Compliance 4
2.3.2 Documentation 4
2.3.3 Types of changes 4
2.3.4 Authorisation Responsibilities 5
2.3.5 Handling changes 5
3. VALIDITY AND DOCUMENT MANAGEMENT 6
4. RELATED DOCUMENTS 6

1. Purpose, scope and users

The purpose of this policy is to ensure that changes to Credit Union (CU) are managed through an established process.

This policy applies to all Credit Union full-time, part-time and contracted employees, vendors and suppliers involved in activities that use or manage technology solutions within CU.

Users of this document are employees, directors and volunteers within CU.

2. Policy

The Change Management process manages the lifecycle of all changes, enabling changes to be made without disruption of IT services. A change is any addition, modification or removal of anything that could have an effect on IT services.

2.1 Scope and goals of Change Management process

The scope of the Change Management process covers:

- Services (new or changed)
- Management information systems and tools
- Technology architecture
- Processes
- All documents used by CU to support IT Management
- All configuration items and implications

Goals of the Change Management process are:

- To ensure that changes are documented, evaluated and, for authorised changes, that they are planned, prioritised, tested, implemented and documented
- To ensure that all changes to critical configuration items are documented

2.2 Unauthorised changes

Credit Union prohibits unauthorised changes. Non-compliance and any failure to observe the policies contained in this document will be subject to the organisation's disciplinary procedures.

2.3 Process guidelines

Changes significantly influence operational services and respective business processes. Therefore, setting up a Change Management process considers the following parameters to control and decrease the level of risk.

2.3.1 Compliance

The Change Management process considers the following regulatory, i.e. legislative requirements:

- The Credit Union Act 1997
- Data Protection Act 1988
- General Data Protection Regulation (EU Data Protection Directive)

2.3.2 Documentation

Other than pre-defined standard changes/standard support every change is triggered by a Request for Change (RfC) document (see Request for Change and Change Record in Supporting Documents).

Standard changes are pre-approved and do not require authorisation prior to initiation.

They must however be logged internally in the Change Log for auditing and change control purposes.

2.3.3 Types of changes

Credit Union defines the following types of changes:

- Standard Change
  A pre-authorised change that is low risk, relatively common and follows a prescribed procedure. This type of change is usually carried out as part of a normal service or support request e.g. reset a password, troubleshoot network or application issues, standard software support.

- Normal Change
  A change that is not a major or a standard change. This type of change will require need the approval of a member of the Management Team. A normal change refers to changes that must follow the complete change management process. Normal changes are categorised according to risk and impact to the organisation/business. For example, normal change – low risk and impact, medium risk and impact. Examples are new user setup, PC set up, change of access controls and permissions for users on network or within applications, change of business rules, system parameters.

- Major Change
  Major changes will be required to follow the complete change management process, must complete an assessment of the impact of the change and business case where new hardware, IT services, or software are to be introduced and must obtain Management Team approval. A major change will be defined as high risk and impact. Examples are new hardware, new systems and software, introduction of new service providers or technology that will require access to or integrate with CU's IT network and software systems.

- Emergency Change
  A change that requires urgent action to avoid impacting the normal business operations to a high degree or to protect the organisation from a security threat. This type of change must obtain prior approval from two members of the Management Team.

2.3.4 Authorisation Responsibilities

All normal, major and emergency changes must be authorised. Credit Union uses the following authorisation model:

Type of change	Authorised by (Change Authority)
Standard	Pre-authorised
Normal	Member of Management Team
Major	Board of Directors
Emergency	Minimum two members of Management Team

2.3.5 Handling changes

The CEO/Compliance Officer is responsible for:

- Defining and agreeing the time frame for Major and Emergency changes
- Verifying implementation of changes.

- Reviewing changes [monthly/quarterly] to identify trends and possible improvements.
- Remediation – ensures that actions that have to be taken in case of unsuccessful changes to restore normal operations of the services(s) are set.
- Documenting and agreeing on the approval process for Emergency changes and the procedure for handling these.

Major changes are changes with significant organisational and/or financial implications that could impact both front and back office operations and services adversely. These are handled in the following way:

Besides the RfC, a Change Proposal (see Change Proposal in Appendix) must exist for major changes. A Change Proposal is prepared by the CEO with the authorisation of the Board.

- All Major system and software development (new services and modules, significant version upgrades) must follow recommended practices and CU's Change Management Policy. This includes but is not limited to:
    - Preliminary Analysis including requirement gathering of both business and technical information
    - Where a significant change is being evaluated a Business Case and Risk Assessment must be prepared
    - IT Due Diligence must be completed
    - Network Security and Cybersecurity implications and risks must be documented
    - System testing and User testing including user acceptance must be completed
    - User training must be completed
    - Post implementation reviews must be completed
    - Documentation on the solution and data flows must be completed
    - On-going support and maintenance must be documented
    - All testing must be performed on a test and/or quality assurance system prior to live implementation
    - All development must follow the change management policy of this organisation

The Emergency Change Team is used to authorise Emergency changes, and consists of the following members: [CEO, Deputy CEO /Management Team]

The Emergency Management Team is chaired by CEO.

A change review process is completed quarterly by the Compliance Officer. This will require an audit of change requests, approvals, record keeping and vendor records.

3. Validity and document management

This document is valid as of [date].

Owner of this document is the CEO who must check and, if necessary, update the document at least once a year.

4. Related Documents

Appendix 1: Change Management Request Form

Appendix 2: Change Record Log

Appendix 3: Business Case

Change Management Request Form

Change Description/ Change Request Filename:			
Change Request No.:		Project:	
Requested by:		Date:	
Department		Telephone:	
Description of the change:			
Change needed by (date):			
Reason for the change			
Requested by:			
Approval of Request:			

Change Impact Evaluation					
Change Type		Application		Database	
		Hardware		Procedures	
		Network		Security	
		Operating System/Utilities		Schedule Outage	
Change Priority		Urgent	Change Impact		Minor
		High			Medium
		Medium			Major
		Low			
Environment(s) Impacted:	*ICE, Online Member Services, Finance, EFT Processing, Connectivity*				
Resource requirements: (personnel, h/w, s/w)					
Test Plan Description					
Rollback Description	.				

Change Approval or Rejection				
Change Request Status		Accepted		Rejected
Comments:				
Change scheduled for (date):				
Implementation assigned to (names):				
Change Control Sign off:	*Management Team Member, Two members of the Management Team, Board*			

Change Implementation			
Staging test results:			
Implementation test results:			
Date of Implementation			
Implementer Sign Off		Date	