

Change Management Policy

**Document Statistics**

|  |  |
| --- | --- |
| **Type Of Information** | **Document Data** |
| Document Title | Change Management Policy |
| Document Code | PO/CMPO/V02 |
| Date of Release | 27th Dec 2023 |
| Document Revision No | 2nd Release of document |
| Document Owner | IT Executive |
| Documents Author(s) | IT Head |
| Document Change Reviewer | IT Head |
| Security Classification | Confidential |
| Document Status | Approved |

**Document approvers.**

|  |  |  |
| --- | --- | --- |
| **Sr. No** | **Approver** | **Approver Contact(Email)** |
| 1 | Vice President Strategy & BIS | Rashmin Vyawahare <r.vyawahare@cloudextel.com> |

**Document Change Approvals**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version No.** | **Revision Date** | **Nature of Change** | **Date Approved** |
| 1 | 29th July 2022 | Initial Release | 28th July 2022 |
| 2 | 25th Dec 2023 | Revised Release | 27th Dec 2023 |

**Document Contact Point**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr. No.** | **Document/Process** | **Document Author** | **Document Primary Focal Point** |
| 1 | Change Management Policy | IT Head | IT Policy Folder |

**Document Reference List**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr. No** | **Reference No.** | **Document Name** | **Effective date** |
| 1 | PO/CMPO/V01 | Change Management Policy | 29th July 2022 |
| 2 | PO/CMPO/V02 | Change Management Policy | 27th Dec 2023 |

**Index**

Contents

[1. Purpose 5](#_Toc164953823)

[2. Scope 5](#_Toc164953824)

[3. Abbreviations and definitions 5](#_Toc164953825)

[4. Guidelines 6](#_Toc164953826)

[5. Policy details 6](#_Toc164953827)

[5.1 Recording Changes In Change Request Forms 6](#_Toc164953828)

[5.2 Change Management Committee 7](#_Toc164953829)

[5.3 Approval Of Change Requests 7](#_Toc164953830)

[5.4 Executing and Testing Changes 8](#_Toc164953831)

[5.5 Change Management and Documentation 8](#_Toc164953832)

[5.6 Unscheduled/Emergency Changes 10](#_Toc164953833)

[5.7 User ID and Access Changes 10](#_Toc164953834)

[5.8 Hardware Changes 10](#_Toc164953835)

[5.9 Operation System and Application Changes 11](#_Toc164953836)

[5.10 Patch and Service pack management. 11](#_Toc164953837)

[5.11 Addition of hardware/Software and any other IT resource 12](#_Toc164953838)

[6. Measurements 12](#_Toc164953839)

[7. Objective Evidence 12](#_Toc164953840)

[8. Flow Chart 13](#_Toc164953841)

# Purpose

Changes to Excel Telesonic India Pvt Ltd’s information technology facilities and systems must be controlled in order to ensure that changes made to operational components are applied in a controlled and consistent manner.

# Scope

This policy applies to all temporary Staff, Employees, Process Owners, Clients using Excel Telesonic India Pvt Ltd’ computing resources. All are expected to be familiar with and comply with this policy. All locations and processes within the scope of ISO27001 are covered by this document.

The change management policy will be applicable to systems and information processing facilities, and would include but not be limited to:

* + - Changes to hardware and software configurations.
    - Changes to operating systems and operating system configurations which must include application of patches and service packs, configuration changes, and version upgrades.
    - Changes to application software programs and application or database software configurations which must include application of patches, configuration changes, and version upgrades.
    - Changes to network and communication device configurations; and
    - Changes to configuration of physical access and environmental control devices. Exclusion: Configuration changes that are declared as standard operating procedures by manufacturer.
    - Changes in source code.
    - Additions of new location/new application/new Hardware to the existing setup
    - Changes in the access authorizations will be covered in Logical Access Controls
    - All other changes to the critical systems will be covered under the change management system.

**The Change Management policy addresses the following**:

* Recording changes in change request forms.
* Approval of change requests.
* Impact assessment due to the change.
* Executing and testing changes.
* Rollout procedures
* Documentation of changes.
* Unscheduled/Emergency changes

# Abbreviations and definitions

|  |  |  |
| --- | --- | --- |
| **Sr. No** | **Abbreviation/Definition** | **Explanation** |
| 1. | IT | Information technology |

# Guidelines

Not applicable

# Policy details

## Recording Changes In Change Request Forms

Change request forms shall be used to request any change in system or information processing facilities as mentioned in the scope.

The change request form shall record details like Name of the change requestor, department, location, system in which change is requested, reason for change request, systems that will be affected by the change etc.

The change request forms shall be kept as records along with other documentation related to a particular change.

## Change Management Committee

A change management committee meets monthly depending upon the volume and complexity of changes to be reviewed that have been carried out in that particular month.

For critical and complex changes the Change Management Committee should review and approve the change before the change is carried out.

Representation in the change management committee is dependent upon the functionality of the specific application. For example, if the application impacts financial processing and reporting or regulatory compliance, representatives from finance and compliance departments should be invited to participate in the change management committee meeting.

A unique change management committee does not need to exist for each application—if appropriate, a change management committee may review all requested changes for several applications that reside in the area of responsibility.

If approved by the change management committee, the change request is assigned to a release under the management of a project or product manager and systems development resources are assigned to the request to make the appropriate application system change.

## Approval Of Change Requests

Any change requested must be approved by approving authority, based on business requirements. This request will be forwarded to IT Head which will forward the request post validation to the change request handling team from the concerned department or ask for more clarifications from the end user.

An assessment of the proposed system changes must be performed to assess its potential impact on Excel Telesonic India Pvt Ltd’ computing systems before its approval.

## Executing and Testing Changes

All critical and complex changes must be tested before being carried out in the live/production environment, wherever required.

Changes should not be carried out in production environment directly if development/ test environment is available.

A quality assurance test of the changes to be implemented must be performed in a test environment prior to implementation in the production environment.

A backup of the system impacted by the change must be made prior to its being updated.

For critical systems, rollback, and recovery procedures in case of unsuccessful changes must be followed.

CloudExtel recognizes the importance of effective change management practices to minimize the risk of disruptions to critical systems. In addition to implementing changes according to established procedures, it is imperative to have a documented rollback strategy in place to swiftly recover critical systems in the event of an unsuccessful change.

**Rollback Strategy:**

In the event of an unsuccessful change that adversely affects critical systems, CloudExtel has a documented rollback strategy in place to swiftly revert to the previous state. This strategy outlines the steps and procedures required to initiate the rollback process, including:

* Identification of the failed change and impacted systems.
* Activation of predefined rollback procedures to restore systems to their last known stable state.
* Validation of the rollback process to ensure successful restoration of functionality.
* Communication of the rollback activities to relevant stakeholders.

## Change Management and Documentation

The change management process must involve documenting and managing the change requests.

The documentation must provide for a brief description of the changes requested, the date on which the request was made, prioritizing of the request, tracking, and controlling modifications and assigning a unique number to each request.

All changes must be scheduled, and all the affected parties must be informed in advance of the change.

Updating the database need to be done after implementing the change All changes have to be reviewed after the roll out.

## Unscheduled/Emergency Changes

Unscheduled/emergency changes must be carried out only in case there are critical production issues, which require the change to be carried out.

Any unscheduled changes must not be done without proper approval.

An audit trail of the emergency activity must also be generated which logs all activity, including but not limited to:

1. The user-ID making the change.
2. Time and date
3. The commands executed.
4. The program and data files affected.

After unscheduled changes are carried out, normal change procedures must be expedited.

## User ID and Access Changes

Any changes to user id including changes to the authorization levels must be done by following the procedure defined in Access Control policy.

The change must involve raising a request and approval of the same by his/her supervisor as well as from the Head of Department (HOD) of the person requesting access.

All changes must be documented, and a trail must be maintained by means of preserving the change requests.

## Hardware Changes

Any changes to hardware must be done by following the change management process which includes raising of change request, approval by the appropriate authorities and documentation of the same.

If hardware is available in stock for request raised, then the request is closed within 2 working days. In case of shortage in stock necessary approvals are sorted from IT Head and requisition form is filled. On receipt of necessary approvals including the quotations rates the request is closed within 15 working days.

The custodian of the hardware must conduct all the hardware changes after due approval of the change.

Changes done to the hardware must be updated in the hardware/Asset register after the change is made.

Changes done to the hardware must be monitored after the change to ensure that there is no untoward affect due to the change.

## Operation System and Application Changes

Any change to the operating system or application must be strictly controlled by the use of the change management process, which will include raising of change request, testing, approval by the appropriate authorities and documentation of the same.

Changes to the operating system or the application must be done by following the steps mentioned in the documented operating procedures, wherever applicable.

All changes must be documented, and a trail must be maintained by means of preserving the change requests.

Any change that involves downtime or disruption of services must be done after giving an appropriate notification to the affected users by email.

## Patch and Service pack management.

Operating systems will be periodically updated with the new release or patches from the vendors. New releases/ Patches pertaining to the operating system will be tested before being implemented in production environment to ensure that there is no adverse impact on operation, application controls or security.

Application of patches must be done in a controlled manner.

A patch or service pack must be applied only when it is a critical patch or there is a requirement for the application of the same.

Only tested versions of the patch or service pack must be considered for application, wherever needed.

The patch or service pack must be obtained directly from the vendor or downloaded from the vendor site only.

A test bed must be prepared to simulate the actual production environment and the patch or service pack must be installed in the testing environment. The environment must be monitored for performance and other issues.

On successful testing by the functional users, the patch must be applied on the production systems.

For desktop related patches, the application must be done in a scheduled manner using change request form.

## Addition of hardware/Software and any other IT resource

All hardware or any other resource addition or removal of it from the production environment would be controlled and approved and a complete track of it maintained to ensure non-disruption to the operating environment.

# Measurements

NA

# Objective Evidence

The change management logs are maintained on Teams (SharePoint)

# Flow Chart

Change Request Information Repository

End User Validated Change Control Request Information

Yes

Change Approved?

Change Request Information Repository

No

Change Control Repository

Change Request Information Repository

Change Request Information Repository

Perform User Acceptance Test

Change Request Information Repository

Change Request Information Repository

Signify Approval of Changes

Update Change Request to Signify Application of Changes

Validate Change Request

Change Request

Change Management Commitee

IS/Application Support

End User

Close and Archive Change Request

Validate Production Move

Migrate Changes to Production

Apply Changes to System

Close Change Request, Communicate Disposition to End User

Reflect Approval in Change Request Information, Assign to Release if appropriate

Update Change Request to Signify Application of Changes

Document Change Request

|  |  |  |
| --- | --- | --- |
|  | Create Production Change Control |  |