Recite me

Change Management Policy

www.reciteme.com

Version	Date	Details	Author
1.0.0	22/02/2022	Initial Version	Craig Tyers

Table of contents:

Introduction:

Purpose:

This document outlines Recite Me’s Change Management Policy across our organisation.

In order to maintain security, availability and integrity of IT systems, we require a robust and mandatory Change Management Policy.

This Policy will apply to required amendments, enhancements and changes to existing systems and services, as well as the introduction of new services.

This Change Management Policy sets out the required processes and procedures for the implementation of any such changes..

Scope:

Business wide. All changes, new services, enhancements or amendments to any IT systems or services which Recite Me manages, must be subject to the Change Management Policy procedures.

Definitions:

Change Owner:

A Change Owner is a staff member (or group thereof) who made a Change Request. It is the Change Owner(s) responsibility to fully detail the Change Request in order to put it to the Change Management Team.

Change Request:

A Change Request is a request (formal or informal) to update, alter or replace any aspect of any system within the Recite Me IT infrastructure.

Change Management Team:

The Change Management Team membership will be dependent upon the initial Change Request. Any member of the Recite Me IT, Development, and Dev-ops team who may be responsible for approving or making changes to an affected IT System, will be required to be part of the Change Management Team for the requested change.

Change Manager:

On a per request basis, the Change Manager is the single point of contact for the change: they are responsible for identifying all affected systems and the staff members who represent those systems (and should therefore choose the Change Management Team). The Change Manager is responsible for overseeing the change to completion (either live state, denial of change, or rollback in the case of a failed change)

Change Time Frame:

Agreed before a Change Request is approved, the Change Time Frame identifies the time period in which the change can be actioned.
This should be sufficient time to allow for the action, testing and potential rollback of the change. It should forecast sufficiently far ahead so as to allow communication of the expected Time Frame to those who may be affected by the change, or the change process.

Action Plan:

Agreed before a Change Request is approved, the Action Plan should identify each member of the team that is required to action a change for this Change Request. It should detail any steps to be taken (including preparing any backups necessary) and serve as a checklist to make sure that the Time Frame, identified actions and team members are appropriate and available.

Test Plan:

Agreed before a Change Request is approved, the test plan should identify the team member(s) responsible for testing the state of the change after it has been actioned. The Test Plan should detail any steps that the testers should follow and the communication protocol to follow should any test be considered a fail. The test plan should also specify the testing time frame (following the Change Manager communicating to the testers that the action plan has been completed).
Finally the Test Plan should detail the process for validating and communicating that the change was successful.

Rollback Plan:

Agreed before a Change Request is approved, the Rollback plan should identify those team members responsible for performing system rollbacks following a failed Change Request. It should detail the rollback process and expected time frame for the Rollback to occur, as well as the communication protocol to follow when the process is complete.

Communication Plan:

Agreed before a Change Request is approved, the Communication Plan should identify all affected users and their user type (Client/Developer/System Administrator/etc). It should set out the plan to communicate with each of these user groups throughout the Change Request, the Change Timeframe and the success/failure of the change. The Communication Plan may involve the Communication and/or Marketing Team(s) updating clients of updates or changes to our systems, and as such must not be overlooked.

Policy Statement:

This policy outlines the process for submitting, reviewing and approving or denying technology Change Requests.

Submitting a Change Request:

A Change Request can be submitted formally (in writing with supporting documentation) or in-formally (verbally with supporting argument) to any member of the Change Management Team (see *Responsibilities*). The request should be sufficiently thought through by the requester so that it's implications, (both positive and negative, and also if approved or denied) are fully understood and communicated at the request stage.

The team will need to understand:

- What is the change being requested?
- What are the business and technological implications of making the change?
- What are the business and technological implications of not making the change?
- What systems will be affected?
- What the Rollback procedure will be?
- How to test and identify a successful or failed change?
- The proposed change Timeframe?
- How to communicate the change time frame and success or fail state

The Change Request should identify any impacted areas of the IT infrastructure and make sure to highlight the implications to those areas to the appropriate team members (see *Responsibilities*)

The Change Request should also include consideration for a Rollback Plan.

Additionally the request should consider and provide a plan for the roll out of the change, including any required down time or system depreciation.

Once Submitted, the Change Management Team may request further investigation and/or formal documentation from the submitter(s).

Reviewing a Change Request:

Reviews for a Change Request should happen across all potentially affected systems, and should be the roles of those members of staff responsible for maintaining those systems.

It is the responsibility of the Change Manager to identify and involve all those members of the team which may be responsible for systems that the change could affect.

As soon as any system that a particular member of the team is responsible for maintaining becomes affected by a proposed Change Request, that team member becomes part of the Change Request's Change Management Team; they are thus responsible for assessing the impact of the requested change on the system they maintain.

The change should be reviewed for worthiness by all affected system maintainers, as well as assessed for potential risk or unforeseen effects.

Only when a Change Request has successfully been approved by representatives of all affected systems can that request move forward.

Should any team member raise any concerns as to the change, its impact, or affect on the systems, or the proposed Rollback strategy then the request should be denied.
The Change Owner(s) should then address the raised concerns if they wish to re-submit the Change Request.

Denying a Change Request:

Once the Change Manager has identified and involved all team members who are responsible for maintaining any system that may be affected by a Change Request, the original request, together with any pertinent documentation, should be put to those staff members for approval.

Should anyone raise any objection to any aspect of the Change, Rollback or Communication Plans for the requested change, the Change Request should be denied.

Once denied, a Change Request should be returned to the Change Owner with the reason(s) for its denial.

The Change Owner can then amend or update the request to consider the feedback.

Approving a Change Request:

A Change Request should only be approved once all affected system representatives have received full explanations of the requested change and its implications. Those team members must have agreed that the request does not pose any security or integrity issues and that the proposed Timeframe, Action Plan, Rollback Plan, Test Plan and Communication Plan are all acceptable.

At this point it is important to consider the application of the change- Identify the staff member(s) responsible for performing (Actioning) the change and the action plan.

A Change Request can only move to the ready to be actioned state once it is approved by the Change Management Team and has each of the following in place:

- Action Plan
- Test Plan
- Rollback Plan
- Communication Plan

The Change Manager should be fully satisfied with all of the above before a time frame for actioning the change is set.

If the Action Plan necessitates down time or other deprivation of services this should be communicated to the wider business and system users before the change is made; this must include sufficient warning to allow for those affected to make alternative arrangements (this time frame may vary on a per case basis).

Only once a request is approved, communicated and any mitigations in place should the request be actioned.

The Change Management Team is now responsible for identifying the team member(s) responsible for actioning the change and should, with input from those team members, agree on a suitable time frame in which to perform the change.

Actioning a Change Request:

As part of the approval process, each team member who is responsible for actioning the change will have been identified and a suitable time frame for making the change agreed.

At the agreed time the change can be performed. Any backup operations mandated by the Rollback Plan for the Change Request should be included as part of the Action process.

Once actioned, the actioning team member(s) are responsible for communicating the action status to the Change Manager.

The Change Manager is then responsible for testing (or identifying the team members best placed to test) the change for success; this should happen as soon as feasibly possible following the change.

The Change Request can only be considered complete once tested by the Change Management Team and agreed that the change has been applied without any issues (or with issues that were successfully mitigated as part of the request).

Rollback Plan:

The Rollback Plan for any Change Request should be well communicated with all team members involved in the request's approval, or action.

Should the Change Manager be unable to fully satisfy themselves (or any member of the Change Management Team) that the change has been successful, it will be deemed to have failed.

A failed change should move straight to the Rollback Plan defined for the Change Request, the team members identified as responsible for actioning the Rollback Plan should all be informed and the procedure initiated as soon as is reasonably possible.

At this stage the failed change is closed and should be passed back to the Change Owner with a full explanation of the issues faced during rollout, and the cause for rollback.

The Change Owner can then re-assess the Change Request and re-submit an amended request.

Documentation and Communication:

The updated system(s) and the new state should be fully documented and communicated to all.
It is vital that any member of staff who may interact with a system that has been changed is aware of, and fully briefed on, the change.

Assuring that this communication takes place is the responsibility of the Change Manager.

In the case of a system change that may affect service users/clients the communication requirements increase exponentially.

As detailed in the approval process, any change that may cause a change to users should be communicated to those users in sufficient time to allow the users to adapt to the change, or prepare mitigation strategies.

When a change affects external clients the Change Manager should involve the Communication and/or Marketing Team(s) in order to convey the message appropriately.

Responsibilities:

Change Owner:

The requestor(s) of a change. It is the Change Owner's responsibility to fully plan and consider all implications of the requested change.

To communicate the request to a Change Manager.

Additionally a Change Owner should consider the Action Plan, Rollback Plan and Communication Plan for a Change Request; these will also be considered together with the Change Management Team during the approval process.

Change Manager:

The Change Manager is responsible for identifying the areas/systems that a change may affect, and therefore for appointing a Change Management Team for the Change Request. (The Change Manager should be the staff member most appropriate for overseeing the whole Change Request).

Additionally the Change Manager is responsible for overseeing the Action Plan and Communication Plan, as well as recognising any testing post action of the change that may require Rollback, and for overseeing said procedure.

Change Management Team:

Consisting of team members representing each of the affected systems identified in the Change Request, the Change Management Team are responsible for identifying any risks or unforeseen effects of the affected change, for (together with the Change Owner) implementing an Action and, if required, the Rollback Plan(s), and proposing a Communication Plan and Time Frame for the change.

Change Actioner(s):

Consisting of team members identified in the Action Plan as responsible for actioning the change. Responsible for following the action plan and the appointed Time Frame and communicating the status of the action plan to the Change Manager

Testers:

Identified by the Test Plan, responsible for testing the actioned change and reporting its success (or otherwise) to the Change Manager.

Rollback Performers:

Identified in the Rollback Plan, these people are responsible for implementing the Change Request's Rollback Plan should an actioned change fail during the Test Plan, and communicating its success to the Change Manager. These may be the same as the original actioners, a different team of people altogether, or some combination thereof.

Communication Team:

Identified in the Communication Plan, these people are responsible for communication of the upcoming change and change Time Frame to all interested parties. They are additionally responsible for implementing the post-action Communication Plan to all affected parties once instructed to do so by the Change Manager.

Change Types:

Standard Change:

This type of change is one that is considered to be part of a team members' daily routine.
Such as a content update, or release to a development environment.
These changes are not included in the Change Management Policy and are instead considered part of Standard Operating Procedure.

Emergency Change:

An Emergency Change is a response to a failure, error or new information which puts one of our systems at risk.
An Emergency Change should follow the change policy where possible, however may be expedited with a smaller Change Management Team, and by post-change communication in lieu of informing affected users.

It is, however, important that even Emergency Changes are not just implemented when the issue is discovered, but are instead implemented with a proper Test and Rollback Plan in place. Even in an emergency, it is vital that these systems are maintained in a manner that allows us to keep track of, and, if necessary, reverse, any changes.

Major, Minor, and Significant Changes:

A Major, Minor or Significant Change must follow the change policy in full.
The Change Management Team must agree fully to the Change Request before it is approved: Action, Test, Rollback and Communication Plans must be in place.

The Change Management Team should be of suitable size, experience and of sufficient system knowledge to approve the level of change required.

At the judgement of the Change Manager, a Significant Change may require a more formal approach with a larger team and individual responsibility for each of the steps in the process being formally identified and documented.

A Minor Change, may, again at the Change Manager's discretion, be suitable for verbal-only planning, fewer team members involvement and there-by a quicker turnaround.

Breaches:

Breaches of this policy are to be taken very seriously and may result in disciplinary action.

Additionally, identification of breaches should trigger a review and a re-communication of this policy to all staff members who would be responsible for making or implementing Change Requests.

Review:

This policy will be reviewed following any substantial changes to infrastructure or related business policies, legislation changes and or any non-compliance prompts. The document will be automatically reviewed after annually.