CHANGE MANAGEMENT PROCESS

*s*

*Effective Date: ddmmyyyy*

*Classification: INTERNAL*

**INTERNAL INFORMATION**

This is a proprietary document and is the property of XXXX.; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX.

Table of Contents

1. Introduction 3

2. Scope 3

2.1 Normal Changes 3

2.2 Major Changes 3

2.3 Emergency Changes 4

3. Software Development 4

4. Change Management Process 5

4.1 Process Narrative 6

4.2 Information to be supplied on change requests 7

4.3 Assessment of Changes 7

4.4 Approval of Changes 7

4.5 Deployment of Changes 7

4.6 Process Roles and Responsibilities 8

4.6.1 The Change Manager 8

4.6.2 ISO – Information Security Officer 8

4.6.3 The Change Initiator 8

4.6.4 (Emergency) Change Advisory Board (CAB) 8

4.6.5 Change Implementer 9

4.7 RACI (Responsible Accountable Consulted Informed) Matrix 9

5. Procedural Steps for Users 10

6. Enforcement 10

7. Document Management 10

7.1 Document Revision Log 10

7.2 Document Ownership 10

7.3 Document Coordinator 11

7.4 Document Approvers 11

7.5 Document Distribution 11

# Introduction

The purpose of this document is to set out the XXXX process of change management. The objective of this process is to ensure that changes to IT services and their associated components are recorded and then evaluated, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner.

A change request may arise for many reasons, including the following:

* An incident or problem
* New hardware installation
* New functionality
* IT Infrastructure upgrades
* New or changed legislation
* Changed business requirements or direction
* Retirement of service

A change request must be assessed for impact (including information security implications) and resource requirements before being considered, depending on the category, by the Change Advisory Board (CAB). To assist with impact assessment, the identification of related systems/components affected by the proposed change and also input from other affected support groups may be required.

After assessment, if the change is deemed acceptable it will be authorised by the Change Manager or CAB. Once implemented the change will be reviewed and subject to the findings of the review, closed.

# Scope

The intended scope covers all of the XXXX's computing systems, platforms and their primary functional components.

Categories/Types of Change

The following categories of change will be used:

* Normal
* Major
* Emergency

## Normal Changes

These are ‘business as usual’ changes which are expected to make up majority of the change requests that are logged and handled through the change management process as described in this document. They are low impact and low risk changes. Normal changes will be approved by the Change Manager. See Roles and Responsibilities below.

## Major Changes

Major changes will be logged within the change management process, approved by CAB and may then be referred to the IT Steering Committee for authorisation as their scope and implications will generally encompass a wider audience with high risk. They will then be raised as projects with their own business case, project team and budget.

However, note that a project may generate further change requests that may be managed within the change management process as normal changes.

## Emergency Changes

Whilst all changes likely to be required should be foreseen and planned, there will be occasions when business requirements demand that changes be made in an emergency situation. Such changes are those requests which impact on internal or external ‘live’ systems and require implementation in order to resolve (or prevent) a current high priority incident or problem. In such cases a change request must be raised immediately even if the full change details are not available and the CAB must be notified. This is to ensure that all parties are aware at the earliest opportunity.

From initial logging of the change, the principles of the normal change management process should be observed as far as is realistic, however, as an emergency changes may require swift approval from the CAB an Emergency CAB (E-CAB) meeting may be held.

If an emergency change cannot be formally authorised after reasonable efforts have been made to follow the process (e.g. out of hours) a local decision, by the Change Manager and System Owner, may be made as to whether this change will be implemented. Urgency, impact and risk(s) of not applying the change should be considered and documented.

Urgency, impact and risk of not applying the change will be considered before implementing the change. However, details of the change must still be recorded, and the change management process followed retrospectively to ensure that records are maintained accurately, and the success or failure of the change can be reviewed.

Where timescales allow it, the Change Manager in collaboration with the relevant support groups will ensure the following:

* Sufficient staff and resources are available to action and support the change request
* Back-out plans have been documented and passed to the change Implementer
* As much testing as possible of the emergency change has been completed
* A full risk assessment of the change has been made and documented before execution

When an emergency change request is logged the Change Manager will do the following:

* Assess who should form the Emergency Change Advisory Board (E-CAB), which should include members of the CAB and the System Owner
* Communicate with each member of the E-CAB by whatever means is appropriate (face-to-face, telephone, email) to obtain a combined impact assessment

The remainder of the process will then continue but under the auspices of the E-CAB rather than the scheduled CAB i.e. as quickly as possible whilst retaining control and managing risk

Changes processed as emergencies will be reviewed by the CAB on a regular basis to ensure that they are genuine emergencies and do not arise from a lack of forward planning.

# **Software** Development

While Software development changes follow the same process outlined in this document however the following extra requirements must be adhered to:

* Every code or software change must undergo a Peer-review process or 4-eye check
* A developer must not be responsible for implementing or promoting their own codes to production.

# Change Management Process



## Process Narrative

The following steps are carried out in the change management process.

| Step | Role | Description |
| --- | --- | --- |
| Raise change request | Change Initiator | Create a change record within Change Management system (ManageEngine) providing all the requested information |
| Classify and Review CR for completeness | Change Manager | The change request needs to be checked that all the required information has been entered. The change should be referred or rejected if it is a totally impractical, duplicate change request or incomplete |
| Amend CR | Change Initiator | The addition of further information if required or classification of existing information |
| Classify and Assess CR | Change Manager | Assess whether the change request is Major, Normal or an Emergency |
| Assess a Normal change request for technical and business risk | Change Manager/ISO | The implications of the proposed change are assessed from a business and a technical point of view. This should include the timing and impact on security, capacity, service continuity plans and release management, amongst other areas |
| Assess a Major change request for technical and business risk | Change Manager/ISO | The implications of the proposed change are assessed from a business and a technical point of view. This should include the timing and impact on security, capacity, service continuity plans and release management, amongst other areas |
| Refer to IT Steering Committee | Change Manager/Change Advisory Board | If the change is categorized as Major according to the criteria specified, then the change will be referred to the CAB or IT Steering Committee if seen as a possible project |
| Assess an Emergency change request for technical and business risk | Emergency Change Advisory Board | The change is assessed as for a major/normal change but in an accelerated timescale either face to face or via telephone, email etc. |
| Approve, reject or refer the change request | Change Advisory Board/ ECAB/Change Manager | Approve if OK, reject if not. Refer back to change initiator if more information required |
| Schedule Change | Change Manager | Inform the change initiator of the result of the CAB and enter the change on the change schedule |
| Prepare and test the change | Change implementer | All changes must be fully tested using the applicable test requirements based on the kind of change done.  Testing should include, but not limited to, User Acceptance, Integration, Stress, Sanity, Unit, Regression, and Functional tests, depending on the type and nature of change involved.  However, test plans, test cases and test scripts, where applicable, should be used and signoffs obtained.  Also, as much as possible deployment into live production must be done gradually after completion of all required tests. |
| Implement change | Change implementer | Make the change on the date and time scheduled. Test to ensure it has worked successfully.  The test outcomes and signoffs will be reviewed by the Change Manager before implementation. |
| Back out change | Change implementer | Remove the change if unsuccessful and roll back to previous settings and configurations |
| Report Success | Change implementer | Inform the change manager that the change was implemented successfully |
| Review change | Change advisory board | Review the change records to ensure that no related incidents or problems have arisen since the change was made |
| Close change as successful | Change advisory board | Close the change with status of successful |
| Close change as unsuccessful | Change manager | Close the change record with a status of unsuccessful |
|  |  |  |

## Information to be supplied on change requests

The following items of information must be supplied on a change request in order for it to be processed and approved. Change request not containing this information will be rejected.

* Initiator name and contact details
* Summary of change
* Change Description
* Business Justification
* Services Affected
* Impact
* Urgency
* Information Security and Data Protection considerations
* Risks and Issues associated with the change – business & technical

## Assessment of Changes

Changes must be assessed from dual perspective of technical and business risk. For many changes this will mean that at least two members of staff will need to be involved – one technical, the other business.

This should include the timing of the proposed change and its potential impact on security, capacity, service continuity plans and release management, amongst others.

## Approval of Changes

The CAB will be responsible for the review and approval of Major change requests. The members of the CAB will be defined as part of the change management process and may vary according to need. The change initiators must not approve their own changes. Where possible the assessors of a change should be different to the approver(s).

Process Outputs:

The outputs of the change management process will be the following

* Closed change records
* Successfully completed changes
* Rejected change requests, where appropriate
* Failed changes, together with relevant reviews and action plans
* Updated configuration item records
* Lessons learned from change reviews
* Closed incidents and problems that are related to the change
* Process roles and responsibilities

## Deployment of Changes

* Where possible, all changes must be deployed out-of-hours when they will have little or no impact to the business.
* After deployment, stakeholders or a selection of users should be engaged to carry out sanity checks to ensure the implementation is fit for purpose. Also, sanity checks on the deployment should also be conducted out-of-hours where possible.

## Process Roles and Responsibilities

### The Change Manager

* Responsible for ensuring that all change requests are managed in line with this procedure.
* Authorizing the transfer from the test environment to the operational (live) environment.
* Provides information regarding the success rates of the process
* Performs the initial check and classification of changes
* Approves low and medium risk changes
* Maintains the change schedule and ensures that all changes are in the correct status

### ISO – Information Security Officer

* Responsible for ensuring information security requirements have been considered in all changes
* Ensure that security tests are carried out for changes prior to implementation.
* Be part of the approving process for the change to be deployed to live

### The Change Initiator

* May be within the business generated changes or within IT infrastructure changes
* Responsible for identifying the needs for a change and providing the required information to allow the change request to be assessed.
* Works with the change builder to define the exact requirements of the change
* May be involved in user acceptance testing of the change once built.

### (Emergency) Change Advisory Board (CAB)

* Reviews and approves or rejects Major/high risk and emergency changes based on the information provided
* Ensuring that all changes to the production environment are adequately assessed for risk avoidance and impact.
* Approving changes presented that meet business needs and conform to change management rules.
* Confirming the priority of authorized changes
* Resolving conflicts in the change schedule.
* Verifying that valid test plans are produced for changes in order to protect the production environment
* Taking corrective action against any person/group who attempts to circumvent the change management process
* Reviewing historical records of changes to ensure that the process is running as required

#### CAB Meetings

The CAB meeting/approvals will be called at the instance of the Change Manager when a change request is received or at least quarterly to review status of previous changes. Four (4) out of the Six (6) CAB members are required to form a quorum and approve or decline changes

The general principle is that all relevant parties are consulted regarding a change that may affect them and these parties may be different according to the scope of a specific change. Therefore, a process of approval via email may be used in advance of a full CAB meeting if the timescale of the change requires a decision before the next meeting.

#### Reports for CAB

The following reports will be produced by the Change Manager on a regular basis and reviewed as part of the CAB meetings in order to identify trends and possible process improvements:

* Number of changes raised and closed within a given time
* Breakdown of categories of change requests raised i.e. Normal, Emergency and Major
* Average time to process a change request of each category
* Percentage successful change requests
* Sources of change requests e.g. business area
* Types of change requests e.g. server, network or by business application

Requirements for further reports will be reviewed on a regular basis. Identified improvements will be input to the continual improvement plan

### Change Implementer

* Works with the change initiator to define the requirements in more detail.
* Creates the items necessary for the change (e.g. new or revised software programs)
* Performs system testing and liaises with the change originator to perform UAT
* Plans the details of the change, test it prior and post implementation
* Provides feedback to the change manager on the status of the change

|  |  |
| --- | --- |
| Role | Members |
| Change Manager | Head of IT or the designate |
| Change Advisory Board (CAB) | ED or designate  CRO or designate  COO or designate  Head IA or designate  Head IT or designate  Information Security Officer  Manager IT & Projects (Secretary) |

## RACI (Responsible Accountable Consulted Informed) Matrix

The table below clarifies the responsibilities at each step using the RACI method, i.e.:

R= Responsible A= Accountable C= Consulted I= Informed

| **Role:** | **Change Initiator** | **Change Manager** | **CAB** | **Change Implementer** |
| --- | --- | --- | --- | --- |
| **Step** |
| Raise change request | A/R | I | I |  |
| Classify and Review CR for completeness | C | R | A |  |
| Amend CR | A/R | C | I |  |
| Classify and Assess CR | I | R | A |  |
| Refer to IT Steering Committee | I | C | R/A |  |
| Assess a Normal change request for technical and business risk | C | R/A | I |  |
| Assess a Major change request for technical and business risk | C | I | R/A |  |
| Assess an Emergency change request for technical and business risk | C | I | R/A |  |
| Approve, reject or refer the change request | I | R/A | R/A |  |
| Schedule Change | I | R/A | I | I |
| Prepare and Test Change | C | I | I | R |
| Implement Change | I | C | A | R |
| Back-out Change | I | A | I | R |
| Report Success | I | A | I | R |
| Review Change | I | R/A | I | I |
| Close Change as successful | I | R/A | I | I |
| Close Change as Unsuccessful | I | R/A | I | I |

# Procedural Steps for Users

1. User logs on the IT helpdesk portal or send a mail to helpdesk@XXXX.com
2. User describes the change on the portal or through the mail
3. A member of the IT helpdesk gets in touch with user to get all the particulars of the change
4. The IT helpdesk staff use the details provided to raise a change request

# Enforcement

All staff of XXXX must comply with all Information Security Procedures. Failure to comply with these procedures may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |

## Document Ownership

This Process is owned by the YYYY

## Document Coordinator

This Process is coordinated by the YYYY

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |

## Document Distribution

Distribution is to all staff