July 2021

BinDawood Holding

IT Change Management Policy

Contents

1 Purpose

IT Change Management policy describes the requirements that need to be performed by the Bin Dawood IT team to effectively manage changes that occur in the IT environment. The objective of the Change Management policy is to ensure all changes are assessed, approved, implemented, and reviewed in a controlled manner.

The goal of this policy is to ensure that changes to production procedures, processes, system, and service parameters are properly managed. This focus will help reduce the risk that modifications, additions, or deletions will negatively impact the integrity, availability, accuracy of systems and data supporting business processes. More specifically, these policies will help ensure that IT:

- Defines and communicates procedures for reviewing, prioritizing, and approving changes driven by business and technical requirements aligned with current and strategic business goals
- Reduces solution and service delivery defects and rework
- Minimizes the potential for a negative business impact due an IT service disruption caused by a change
- Maintains the integrity of information and processing infrastructure
- Maintains acceptable performance of applications and technology solutions
- Understand the impact of Changes on the Service levels

2 Scope

This policy applies to the activity of applying changes to production applications, infrastructure components, management procedures and system settings managed by or on behalf of Bin Dawood IT.

3 Terms and Definitions

Acronyms	Definitions
Change	The addition, modification, or removal of anything that could have an effect on IT services. The scope should include changes to all architectures, processes, tools, metrics, and documentation, as well as changes to IT services and other configuration items.
Change Management	The process responsible for controlling the lifecycle of all changes. The primary objective of Change Management is to enable beneficial changes to be made, with minimum disruption to IT Services.
Request for Change (RFC)	A formal proposal for a change to be made. An RFC includes details of the proposed change and may be recorded on paper or electronically. The term RFC is often misused to mean a change record, or the change itself.
Change Advisory Board (CAB)	A group of people that support the assessment, prioritization, authorization and scheduling of changes. A change advisory board is usually made up of representatives from all areas within the IT service provider; the business; and third parties such as suppliers and service providers.

ECAB	A subgroup of the change advisory board that makes decisions about emergency changes. Membership is limited to key people who are required to take quick decision on Emergency Changes.
Impact	A measure of the effect of an Incident, Problem or Change on Business Processes. Impact is often based on how Service Levels will be affected. Impact and Urgency are used to assign Priority.
Acceptance	Formal agreement that an IT service, process, plan or other deliverable is complete, accurate, reliable and meets its specified requirements. Acceptance is usually preceded by change evaluation or testing and is often required before proceeding to the next stage of a project or process.
Classification	The act of assigning a Category to something. Classification is used to ensure consistent management and reporting. CI's, Incidents, Problems, Changes etc. are usually classified.
Planned Downtime	Agreed time when an IT Service will not be available. Planned Downtime is often used for maintenance, upgrades and testing. See Change Window, Downtime Ex: UPS Maintenance, Data Centre Maintenance, Air Cooling in Data Centre
Back-out	An activity that restores a service or other configuration item to a previous baseline. Back-out is used as a form of remediation when a change or release is not successful.
Configuration Item (CI)	Any component or other service asset that needs to be managed to deliver an IT service. Information about each configuration item is recorded in a configuration record within the configuration management system and is maintained throughout its lifecycle by service asset and configuration management. Configuration items are under the control of change management. They typically include IT services, hardware, software, buildings, people and formal documentation such as process documentation and service level agreements.
Closed	The final Status in the lifecycle of a Change. When the Status is Closed, no further action is taken.

4 Roles & Responsibilities

The people responsible for implementing, changing, enforcing, adhering, and communicating this policy are:

- CTO- Approve and Enforce
- IT Operation Director- Modify, Enforce, Implement and Communicate
- All IT Manager- Enforce, Implement, Monitor and Communicate
- All IT Staff, Change Implementer - Adhere, Communicate
- Change Manager- Review, Enforce, Implement and Communicate
- ECAB- Approve or Reject Emergency Changes

- CAB- Prioritize, Approve or Reject Normal Changes
- Security Manager- Review sample logs against unauthorized changes

5 Change Types

The following is a description of each of the types of changes, its classification, and rules that it should follow. The changes are classified into below changes based on its risk, impact, and urgency.

- **Normal Change** – The changes (RFC) that has significant financial, technical, and business impact and must go through assessment, authorization, and Change Advisory Board (CAB) agreement before its implementation.
- **Emergency Change** – is the highly critical changes needed to restore failed high availability or widespread service failure, or that will prevent such a failure from occurring at that moment, and this change must go through ECAB approval and will be implemented with the highest priority through all its lifecycle.
- **Standard Change** – Used for pre-authorized repetitive, low-risk, often these changes will result from service operational maintenance and will not be handled within the scope of this process. This type of changes will be delegated to Service Desk function to perform and usually handled through the request fulfilment, Access Management, and Incident Management Processes.

6 Change Management Policy

All changes to production environments must be documented, tested, and approved before rolling into production. The change documentation must include below details, at a minimum:

- ✓ Change Type (Emergency, Standard or Normal)
- ✓ Date and time of change,
- ✓ Description of the change
- ✓ Impact of change
- ✓ Affected IT Services, Configuration Items (CIs)
- ✓ Risk of Change
- ✓ Roll-Out Plan
- ✓ Roll-back plan,
- ✓ UAT Results
- ✓ Change approver, Change implementer

- Changes with a significant potential impact to must be scheduled
- Users must be notified of changes that affect the services they are using
- Authorized change windows must be established for changes with a high potential impact.
- Changes with a significant potential impact and/or significant complexity must have usability, security, and impact testing and back out plans included in the change documentation.
- Change control documentation must be maintained in accordance for future reference.

- All application related changes need to be tested in test environment before moving to production environment.
- All changes must be approved as per below approval matrix

Type	Approver
Standard	IT Manager and/or Service Owner
Normal Change	CAB
Emergency Changes	ECAB

- Emergency changes (related to break/fix, incident response, etc.) may be implemented immediately after ECAB Approval and documented retroactively.
- Sample logs of key applications and devices to be reviewed periodically to check any unauthorized changes done without approved RFC.

7 Measures of Effectiveness

Bin Dawood Holding Change Management Policy and process effectiveness will be measured and reported using the below effectiveness which will be measured and reported using the following metrics and measurements:

Metrics	Frequency	Formula	Owner
Successful Changes	Monthly	% of changes successfully processed as planned / Total no of changes	Change Manager
Emergency Changes	Monthly	(Number of emergency changes/ Total number of RFC(s) raised) x 100	Change Manager
Change Control Compliance	Quarterly	(Number of CAB approved changes executed / Total no of changes) x 100	Change Manager
Change Control Compliance	Quarterly	Number of changes without approved RFC/Samples of reviewed system logs to check the changes	Security Manager

8 Related Policy and Processes

- Bin Dawood Holding IT Change Management Process

9 Compliance

Failure to comply with this policy can result in disciplinary action as set out in Bin Dawood Holding general disciplinary policy and when applicable authorities will be notified, and legal action may be taken. Disciplinary action will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets

- Termination of employment/contract
- Other actions as deemed appropriate by Management, Human Resource, and the Legal Department

10 Exceptions

All exceptions to this policy shall be explicitly reviewed by relevant Change Manager and approved by the Chief Technology Officer (CTO). The exception shall be reassessed and re-approved if necessary.

11 Continuous Improvement

This activity serves as a mechanism to continually optimize, refine, and update the policy. This should include meetings of key stakeholders to assess the overall process and various elements of the policy. These assessments should occur yearly at a minimum, as well as after any incidents, audits and consider end users' feedback.