KUOK (SINGAPORE) LIMITED

Change Management Policy

Classification	INTERNAL
Document Reference	ITP0301
Document Version	1.0
Document Status	FINAL

Revision History

Version	Date	Change Number	Summary of Changes
1.0	4 Oct 2022	NA	First copy.

Authors

Name	Title
Foo Tze Uei	Manager, IT GRC

Reviewers

Name	Title
Alan Lee	Senior GM, IT Security and Infrastructure
Han Yong	Head of Technology Solutions
Jonathan Ong	GM, IT Security
Andy Tham	Senior Manager, IT Infrastructure
Eric Huang	Manager, IT Operations

Approval

Name	Position	Signature	Date
Thai Kum Foon	CTO, Group IT	DocuSigned by: F8558A1B4F1B4F4...	04-04-2023

Contents

1 Introduction

1.1 Scope

This control applies to all systems, people and processes that constitute the Kuok Singapore Limited (hereafter referred to as the company) information systems, including board members, directors, employees, vendors and other third parties (hereafter collectively referred to as staff) who have access to these resources.

1.2 Related Documents

The following policies, standards, process or procedures will be replaced and superseded by this document:

- ISMS18004 Change Management Policy

The following policies, standards, process or procedures are related to this document:

- ITS0301 Change Management Standards

1.3 Purpose

The purpose of this policy is to outline change management governance to systematically track and manage a change from start to closure, with the aim to minimize risk to the company.

1.4 Abbreviations

SME	Subject Matter Expert is person who provides the knowledge and expertise in a specific subject, domain or technical area.
UAT	User Acceptance Test is an acceptance test conducted to determine if the requirements of a specification or change meet its intended outcome.
Production	An environment where the service, software, products, or updates are provided to the intended users' usage.
CAB	Change Advisory Board consists of managers and SME who have the capacity and capabilities to assess and make decisions on discussed changes presented.
ECAB	Emergency Change Advisory Board consists of **senior management** who have the capacity and capabilities to assess and make decisions on presented unscheduled/unplanned changes.

2 Policy

General

2.1 Group IT must define and nominate stakeholders that constitute the CAB and ECAB to assess, review and approve change.

2.2 Change to IT systems and applications must be managed in accordance with the company's Change Management standards or process.

2.3 Group IT must define the CAB meeting schedule and frequency. Each CAB meeting must discuss and review all planned changes. All outcome from the CAB meeting must be published to affected stakeholders.

2.4 Change request can only be raised by onboarded staff with an assigned company email account. This staff must also represent the domain where change is affected. Also, change implementor and approver cannot be the same person. This is to safeguard against unauthorised change request or process manipulation.

2.5 Each team must define and maintain their own list of approved standard activities. Each standard activity must have a pre-defined procedure. Use of standard change to perform other types of change is strictly prohibited and will be treated as an unauthorised change.

2.6 All normal or major change must be scheduled and presented to the CAB prior to implementation date or by the stipulated timeline defined in the change management standards for proper resource planning and assessment.

2.7 Unscheduled or unplanned change will be treated as an emergency change and will require ECAB approvals.

2.8 All Major changes must be approved by the Group IT's Senior Management and CAB.

2.9 Emergency change request raised retrospectively must be within 2 working days and ECAB approval must be attached or included as evidence.

2.10 Where possible, all change (except standard and emergency) must be implemented after office hours or during periods where it will not affect the business or operations.

2.11 To minimize change risk, each change must be:

a. impact assessed to determine the risk of the change.

b. where possible, accompanied by a UAT or other test sign-off to ensure change has been tested successfully before it can be allowed to be implemented/deployed into the production environment.
c. supplemented with Implementation plan
d. supplemented with verification plan on how to conduct verification to confirm successful implementation.
e. supplemented with back-out plan to cater for roll-back in case of unsuccessful implementation.

2.12 Post change implementation must be verified by the intended users/requestors. Verification with evidence (i.e. Screenshots, work notes or email) must be provided to prove it is working correctly before request change closure.

2.13 Where possible, each change must be accompanied with a justification. Each stipulated justification must be of relevance, recent date or time, and closely associated with the change. Use of other non-related justification/reference for change is strictly prohibited.

2.14 Change must be implemented within the requested change window and roll back time must also be considered within this period. Any deviation from the change window must be notified to the Change Manager for his awareness and approval.

2.15 Each change request must be represented by the requestor, implementor or technical manager in the CAB meeting for group review and assessment. The CAB reserves the right to approve, reject or request to reschedule the change request.

2.16 Unauthorized change is strictly prohibited and will be subjected to disciplinary actions.

3 Deviation from Policy

In specific circumstances, the applicability of certain Policies and Standards to the company's IT systems and information may require an exemption. Any exception or deviation from Policy and Standards must be duly documented and must be approved by Senior Management.

4 Reporting for Violations

Any violation of this Policy must be reported to the support desk or appropriate IT department

5 Disciplinary Actions

Any staff or other worker of the company found to have violated the provisions of this Policy document may be subject to disciplinary action, including dismissal and legal action.

This page is intentionally left blank