KUOK (SINGAPORE) LIMITED

IT Patch Management Standards

Classification	INTERNAL
Document Reference	ITS0501
Document Version	1.0
Document Status	FINAL

Revision History

Version	Date	Change Number	Summary of Changes
1.0	16 Feb 2023	NA	First copy.

Authors

Name	Title
Foo Tze Uei	Manager, IT GRC

Reviewers

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

Contents

1 Introduction

1.1 Scope

This control applies to all IT information system, servers, applications, and services (hereafter referred to as IT assets), people and processes that constitute the Kuok Singapore Limited (hereafter referred to as the company), 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The following policies, standards, process, or procedures will be replaced and superseded by this document:

- ISMS18015 Technical Vulnerability Management Policy
- SAP-SMP-015-01 SAP Patching Strategy

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

- ITP0301 Change Management Policy
- ITS0301 Change Management Standards
- ITP0501 IT Patch Management Policy

1.3 Purpose

The purpose of this document is to define the IT Vulnerability Assessment and Patch Management Standards of 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.

2 Maintenance Patch Schedule

Domain	Type	Frequency
Infrastructure	Windows	Quarterly
	Linux	Quarterly
	ESXi	Quarterly
	SAN Storage/Switch Devices	Bi-Annually
Network/ Appliances	Firewall	Annually
	Router	Annually
	Switch	Annually
EUC	Laptops/Desktops	Monthly
Application	SAP	SAP-SMP-015-01 SAP Patching Strategy
Application	Non-SAP	As per product roadmap

*Patch Schedule stipulated above may differ due to vendor's patch release date and allowance given for product to be patched up to two generations away from its latest release version in favour of stability except patch deemed to be paramount to security posture (See Section 3).

3 Risk Based Vulnerability Patch/Remediation Schedule

Risk Level	Internal Network Facing	External Network/ Internet Facing
Critical	ASAP or < 14 days	ASAP or < 7 days
High	< 30 days	< 14 days
Medium	< 90 days	< 60 days
Low	< 180 days; Best effort or next version upgrade	< 120 days; Best effort or next version upgrade
Informational	Best effort or next version upgrade	Best effort or next version upgrade

*EUC are excluded and are generally maintained through routine patch schedule as stipulated in section 2 except patch deemed to be paramount to security posture.

4 Deviation from this document

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.

5 Reporting for Violations

Any violation must be reported to the support desk or appropriate IT department.

6 Disciplinary Actions

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

This page is intentionally left blank