



KUOK (SINGAPORE) LIMITED

Vendor (IT) Management
Policy

Classification	INTERNAL
Document Reference	ITP0401
Document Version	1.0
Document Status	FINAL

Revision History

Version	Date	Change Number	Summary of Changes
1.0	10 Nov 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	<div>DocuSigned by:  F8568A1B4F1B4F4...</div>	04-04-2023

Contents

1 INTRODUCTION3

1.1 SCOPE.....3

1.2 RELATED DOCUMENTS3

1.3 PURPOSE.....3

2 POLICY4

3 DEVIATION FROM POLICY7

4 REPORTING FOR VIOLATIONS7

5 DISCIPLINARY ACTIONS.....7

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, and employees. Vendors and other third parties providing IT services or products hereafter collectively referred to as **Vendor**.

1.2 Related Documents

The following policies, standards, process or procedures will be replaced and superseded by this document:

- ISMS21001 Supplier Management Policy

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

- Vendor Evaluation checklist
- Confidentiality Agreement (NDA)

1.3 Purpose

The purpose of this policy is to outline IT vendor management governance in managing and minimising third party risks while ensuring due care is taken before undertaking any contractual agreements.

2 Policy

Vendor Evaluation and Assessment

- 2.1 Selection or evaluation of all vendors must go through Group IT for their assessment and endorsement.
- 2.2 Vendors must be evaluated, and risk assessed prior to the start of any contractual agreement and thereafter on an annual basis. Such assessments also include contracted cloud service vendors or providers (i.e. IAAS, PAAS, SAAS)
- 2.3 A vendor risk assessment must be performed and will be evaluated for their selection. For vendors where products and services are not considered material outsourcing can be omitted.
- 2.4 Each vendor will have a designated point of contact within the company who will be responsible for any escalations or interactions.
- 2.5 Vendors who will be granted access to the company's information and resources must sign the Confidentiality Agreement. However, there may be cases where vendors may insist on using their own agreement, then this must be exercised with caution and must involve KSL Legal perusal prior to agreement.
- 2.6 Vendor whose service relates to processing of the company's information will be required to provide their **active** information security certifications (i.e. DPTM, ISO27001, or SOC2) or be listed in a notable authorised list of certification body or organisation (e.g. Privacy Shield Framework, OSPAR Service Providers).

Vendor Management

- 2.7 Where possible, IT Vendor agreements and contracts must at least specify:
- Scope of work to be delivered;
 - What company information the vendor has access to (if any);
 - How the company's information will be protected by the vendor;
 - How the company's information will be transferred between the company and the vendor;
 - What are the acceptable methods for the return, destruction, or disposal of the company's information in the vendor's possession at the end of the contract;
 - An IT audit process is in place and conducted at least annually;
 - Reporting and communications by the vendor;

ITP0401 Vendor (IT) Management Policy

- Basis of charging;
- Incident response requirements;
- Service Level requirements;
- Contract termination and exit requirements;
- Right to audit vendor or other means of validating quality assurance via industry recognized certifications (e.g ISO27001, SOC2, DPTM, ABS, etc.)

- 2.8 The vendor must notify the company if it sub-contracts any part of the information and communication technology service to another external party; the vendor is required to ensure appropriate information security practices throughout the supply chain. The company holds the vendor accountable for any financial, legal or reputational losses incurred from its sub-contractual arrangements.
- 2.9 Vendor SLA performance must be reviewed periodically or by the frequency as stipulated in the contract. In the event of non-compliance with any contractual agreements such as the SLAs, then regular meetings must be conducted until performance requirements are met.
- 2.10 Any information except aggregated data acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others. The vendor must only use the company's information and resources solely for the purpose of fulfilling their contracted work agreement. Vendor must request permission from the company before using such information.
- 2.11 Vendor must report all related security incidents impacting the company directly to Group IT or appropriate IT channels (i.e. Service Desk) within the timeframe defined in the contract.
- 2.12 Vendors with logical access to the company's information or resources must provide non-repudiation authentication mechanisms.
- 2.13 Where possible, vendor must provide list of personnel working onsite in the company for the contract. Vendor must notify the company and obtain approval for any changes to this personnel list.
- 2.14 Where possible, vendor must establish their business continuity or resiliency plan with the company where it must be reviewed and tested at least annually.
- 2.15 Upon termination, completion of contract or at the request of the company, the vendor must surrender all company's assigned assets (i.e.

ITP0401 Vendor (IT) Management Policy

Company access cards, equipment and supplies) immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized Group IT.

This space is intentionally left blank.

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