



KUOK (SINGAPORE) LIMITED

Mobile Phone Policy

Classification	PROTECTED
Document Reference	ISMS12008
Document Version	2.1
Document Status	Final

Revision History

Version	Date	Change Number	Summary of Changes
1.0	28 Dec 2018	NA	First copy
2.0	02 Mar 2020	NA	Change of Approver
2.1	19 Nov 2020	NA	Change of Approver

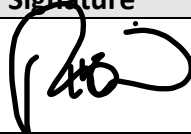
Document Review

Date of Next Scheduled Review
1 st Dec 2021

Authors

Name	Title
Tan Chin Tang	Senior Manager, IT Security

Approval

Name	Position	Signature	Date
Thai Kum Foon	Acting CIO, Group IT		4/2/2021

Contents

1	INTRODUCTION.....	1
1.1	SCOPE	1
1.2	RELATED DOCUMENTS	1
2	CORPORATE MOBILE PHONE	1
3	USE OF CORPORATE MOBILE PHONE	2
4	DATA ROAMING AND INTERNATIONAL CALLING (IDD)	3
5	EMPLOYEE RESPONSIBILITIES	4
6	TERMINATION/TRANSFER OF EMPLOYMENT	4
7	APPENDIX	5
7.1	BILLING	5
7.2	REQUISITION	5
7.3	RE-CONTRACTING OF MOBILE PLANS	5
7.4	REPLACEMENT OF CMP.....	6
7.5	NON-RETURN OF CMP PENALTY	6
	THIS PAGE IS INTENTIONALLY LEFT BLANK	7

1 Introduction

1.1 Scope

This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, vendors and other third parties who have access to Kuok Singapore Limited systems.

1.2 Related Documents

The following policies and procedures are relevant to this document:

- ISMS12002 Mobile Computing Policy
- ISMS12003 Teleworking Policy
- ISMS12004 Bring Your Own Device Policy
- ISMS13002 Email Policy
- ISMS13003 Internet Acceptable Use Policy
- ISMS18004 Change Management Policy
- ISMS18008 Software Policy

2 Corporate Mobile Phone

Corporate mobile phone ("CMP") refers to any portable communication equipment issued by Kuok Singapore Limited to employee for business use. Mobile phones include items such as:

- Smart handphone sets
- Traditional handphone sets

CMP remains the property of Kuok Singapore Limited and its use must be in accordance with the corporate policies.

3 Use of Corporate Mobile Phone

CMPs are intended for business use only. Employees are encouraged to exercise due diligence and operate within the limits under the relevant mobile plans to minimize costs to the Company. Employees should maximize the usage of phone calls from the office phones whenever possible (e.g. using desk phones to make local calls). KCS Group IT will pre-install apps such as Jabber, WhatsApp, Viber, Skype etc on the CMP. Employees are strongly encouraged to communicate through the pre-installed apps under WIFI environment.

CMPs issued to employees are not to be transferred or handed to another colleague, family members or friends for use.

CMP must not be used for the purpose of illegal activities, personal harassment and access to unauthorized websites. Any CMPs used should not contain inappropriate illegal or stolen content.

The employee must comply with the Traffic Police's rules and regulations governing the use of CMP while driving. Each employee is responsible for any fines incurred as a result of traffic regulation breaches. The employee may be warned and subjected to disciplinary actions for such breaches.

The user is expected to take appropriate and sensible precautions regarding the physical security of the device and the security of its data. It is the responsibility of the user to ensure that the CMP's Operating System and its installed applications are patched to the latest available versions, unless instructed otherwise by KCS Group IT.

"Jailbreaking" on iOS devices (or "rooting" on Android device) or any other form circumventing the security features of the operating system (making them vulnerable to compromise), which voids warranties and exposes the Company to other risks is strictly prohibited.

The user is expected to activate and use the operating system's online services to manage the device for features such as locating a missing device, backups and remote wiping (such as iCloud).

All electronic communications, data and records in the CMPs (including pictures taken with the devices) are deemed to be the property of the Company. Transfer of corporate data to any other media other than company approved device is strictly prohibited and is governed by the acceptable use of external data storage device policy.

All mobile devices must be locked with a PIN meeting below requirements:

- Minimum length of 6 digits
- Set idle time-out to 5 minutes maximum (auto-lock)
- Set grace period to 5 minutes maximum (re-enter PIN)

Resigning employees have to release the pin upon the return of the CMP when they return to Group Admin on their last day of work.

4 Data Roaming and International Calling (IDD)

Data Roaming service is activated on all subscribed corporate mobile lines free-of-charge.

The employee who is required to travel overseas must check to ensure he/she is on a data roaming service plan in order to allow the unlimited roaming charges to apply accordingly. i.e. Daily EasyData Roam ("EDR") or Monthly Enterprise EasyData Roam ("EEDR"). If an employee is not sure, he/she must check with Group Admin.

The employee is responsible for reimbursing the company for all charges relating to personal data roaming and voice calls made. The employee must exercise due diligence and operate accordingly under the appropriate circumstances:

- When there are WIFI services available

For voice calls and data roaming, use the pre-installed apps such as WhatsApp, Viber, Skype, Singtel V019 and Singtel ICC etc to communicate. No charges will be incurred.

- When there are no WIFI services available

For voice calls, dial International Dialling Calling ("IDD"). Corporate IDD rates shall apply accordingly.

For data roaming, activate EDR or subscribed to EEDR appropriately. This will help to manage costs.

5 Employee Responsibilities

While the Company respects employees personal time off and does not encourage employees to be working during their annual leave, it is important that employees issued with a CMP remain contactable to attend to business exigencies that require immediate attention or follow up.

It is the responsibility of the user to periodically perform data backups in order to avoid loss of information should the CMP be lost, stolen, corrupted or a device data wipe is required. The user allows the company to remotely wipe the device of all data (including personal data) if:

- it is lost or stolen,
- the user leaves the employment, the company suspects a potential security risk.

The user will inform the company immediately by contacting the KCS Group IT Service Desk if the device is lost or stolen. In the event the device is lost or stolen outside the company's business hours, user will attempt to remote wipe the device themselves via the operating system manufactures online services (such as iCloud) in addition to informing the KCS Group IT Help Desk. The user will supply evidence of a successful wipe to the KCS Group IT Service desk — for example a screenshot of the confirmation, otherwise a second remote wipe will be required.

The user agrees to only use the application stores provided by the operating system manufacturer such as the App Store (Apple), Play Store (Google), etc. Installation of the app from un-trusted sources is forbidden. Although there is no restriction for downloading and usage of applications, employees can approach KCS Group IT for advice on the security risk of using such applications. Any unsanctioned applications may be used at employee's own risk.

6 Termination/Transfer of Employment

Each employee is required to return the CMP and accessories to Group Admin upon termination of his/her employment. Should the employee fail to return the CMP and the accessories, or should the CMP be returned in an unsatisfactory condition, Non-return of CMP penalty shall apply. See Appendix.

Upon termination of employment and at the discretion of the Company, the mobile line may be transferred to the staff who is leaving the Company subject to the approval of the HOD or Director. The transfer fee will be payable by the employee. Company has the right to wipe the data/contacts stored in the CMP.

If an employee gives up the use of a CMP for any reason prior to the end of the 24-months contract period under the mobile plan, the department in which this employee belongs, shall bear the cost of any early termination of the contract. The cost of early termination is stated in the Mobile Service Agreement (MSA).

7 Appendix

7.1 Billing

The Company receives itemised billing for all CMP and these are monitored on a monthly basis by the Department Administrators/HOD. The billings include all calls and data usage incurred by users. Employees are responsible for any personal calls or usage made.

Any discrepancies and charges for personal use, must be declared on the bill. The employee must reimburse the Company within 2 weeks from the date of the bill, for all charges arising from personal usage.

The Company has the discretion to investigate and take appropriate disciplinary action for misuse of the CMP.

7.2 Requisition

CMP is provided to an employee based on the need and job function.

The Head of Department ("HOD") may submit a request for a CMP for use by an employee within his/her department by completing the Mobile Request/ Return Form and submit to Group Admin. This form must be signed and approved.

Under the Mobile Service Agreement (MSA) signed with **the** service provider, Singtel, the models of CMP available are limited to those that are issued as free-of-charge. The CMP will be bundled with standard accessories, including one charger, one battery and one SIM card. Any request for additional accessories requires justification and approval by the relevant HOD.

In the event when there is a preference on the model, specification or capacity of the CMP apart from the \$0 handset provided under the MSA, the chargeable cost of the CMP will be borne by the employee. However, if there is work requirement for a higher capacity, specific model/specifications, then the upgrade cost will be borne by the Company/department.

Group Admin reserves the right to transfer any existing mobile line which may be available for use at that point in time. New mobile lines will be subscribed when there are no available mobile lines for use within the group of companies.

The model/specifications of the CMP will be tested for email set up compatibility by IT before it can be purchased.

7.3 Re-Contracting of Mobile Plans

Mobile phone plans will be eligible for re-contract, subject to the approval of HOD, upon reaching twenty-one (21) months and provided the re-contract will be on the same or higher subscription plan. Otherwise, mobile phone plans can only be re-contracted when reaching twenty-four (24) months.

Group Admin will review and recommend an appropriate mobile phone plan for re-contracting.

Upon re-contract of a subscription plan, employee has to return the existing CMP (with full accessories including original casing, battery, charging plug and cable) in exchange for a new CMP. If the employee fails to return the CMP, a penalty shall apply.

7.4 Replacement of CMP

Each employee is responsible for the safekeeping and proper use of the CMP and ensure that it is in good working condition (fair wear and tear excepted) upon eventual return to the Company. The employee is responsible for the cost of repair or replacement other than fair wear and tear during the period of usage.

Loss of devices must be reported to the Group Admin immediately.

In the event of loss or theft, the employee must call the Corporate Mobile Support CMP hotline immediately to suspend the mobile service to prevent unauthorised usage.

In the event of theft, the incident must be reported to the police within 24 hours. A copy of the Police Report must be submitted to the Group Admin.

If an employee reports loss of his/her, the loss will be investigated by the Company and any further issuance of CMP will be at the discretion of the Company, unless it is due to theft and supported by a police report.

All CMPs are covered with manufacturer's warranty. The warranty period will depend on the brand/model. Terms and conditions of the warranty shall apply accordingly as provided by the manufacturer and this may vary from time to time.

If the warranty period has expired and there are minor parts which require replacements, staff must first approach Group Admin for advice as to the appropriate course of action.

If the CMP fails to operate under the following circumstances, the employee shall approach the respective department for assistance.

7.5 Non-Return of CMP Penalty

If an employee fails to return the CMP for the purpose of re-contracting: or upon termination of employment, or when the job no longer requires him/her to use the CMP, he/she will be liable to pay the below stipulated amount or to replace the CMP with a **similar model/specification** as issued earlier.

Mobile Plan contractual period is between:	Penalty
1 st to 12 th month	\$300
13 th month to 24 th month	\$200
More than 24 th month	\$100

This page is intentionally left blank