



KUOK (SINGAPORE) LIMITED

Acceptable Use Policy
(AUP)

| | |
|---------------------------|----------|
| Classification | INTERNAL |
| Document Reference | ITP0201 |
| Document Version | 1.1 |
| Document Status | FINAL |

Revision History

| Version | Date | Summary of Changes |
|---------|-------------|--|
| 1.0 | 24 Sep 2022 | First copy. |
| 1.1 | 26 Jun 2023 | Added BYOD, improved Social Media and updated Unacceptable use sections. Improved clarity in Section 3 to strengthen governance on personal email, password control, and company data. |
| | | |
| | | |


Authors

| Name | Title |
|-------------|-----------------|
| Foo Tze Uei | Manager, IT GRC |
| | |
| | |

Reviewers

| Name | Title |
|--------------|---|
| Alan Lee | Senior GM, IT Security and Infrastructure |
| Low Han Yong | CIO, Group IT |
| Eric Huang | Manager, IT Operations |
| Jonathan Ong | GM, IT Security |
| Andy Tham | Senior Manager, IT Infrastructure |

Approval

| Name | Position | Signature | Date |
|--------------|---------------|---|------------|
| Low Han Yong | CIO, Group IT | <div>DocuSigned by:  18E59FE427A1465...</div> | 04-07-2023 |

Contents

1 INTRODUCTION3

1.1 SCOPE.....3

1.2 RELATED DOCUMENTS.....3

1.3 PURPOSE.....3

2 POLICY4

GENERAL USE4

SOFTWARE USE.....5

EMAIL USE.....6

SOCIAL MEDIA AND BLOGGING7

ONLINE COLLABORATION SERVICES (E.G. O365, SHAREPOINT, MS-TEAMS, ETC.).....7

BRING YOUR OWN DEVICE (BYOD)7

AUDIT AND INSPECTION8

3 UNACCEPTABLE USE9

4 DEVIATION FROM POLICY 12

5 REPORTING FOR VIOLATIONS 12

6 DISCIPLINARY ACTIONS..... 12

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The following policies and procedures will be replaced and superseded by this document:

- ISMS12004 Bring Your Own Device Policy
- ISMS13002 Email Policy
- ISMS18008 Software Policy
- ISMS24003 IP and Copyright Compliance Policy
- ISMS24006 Social Media Policy
- ISMS12002 Mobile Computing Policy
- ISMS12003 Teleworking Policy

The following policies and procedures are related to this document

- ISMS15001 Access Control Policy
- ITP0201a (External) AUP for Vendors Acknowledgement and Commitment

1.3 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment and/or resources at the company. Inappropriate use exposes the company to risks such as data leakage, compromised security and services, and legal issues.

KCS Pte Ltd. (Hereafter referred to as Group IT) reserves the right to reject any devices deemed unsuitable for accessing the company's resources especially those without adequate security controls implemented.

2 Policy

General Use

- 2.1 Staff must avoid actions and behaviour which potentially compromises the company's reputation, integrity, and business. For example, use of IT resources that may defame, abuse, embarrass, tarnish, or portray the company in false light.
- 2.2 Staff have the responsibility to promptly report the theft, loss or unauthorized disclosure of the company's proprietary information and/or company's assigned assets to Group IT at the soonest possible period from its discovery.
- 2.3 Staff must use IT resources ethically, legally, and consistent with the company's best interests.
- 2.4 The company issued device is for business use only; staff must ensure that it is not to be shared with family or friends or used for personal activities.
- 2.5 Staff must ensure that their assigned mobile devices (i.e. Laptops) are connected to the corporate network on a regular basis to allow latest system patches and malware signatures to be deployed.
- 2.6 Do not leave computing device unattended, especially in public view, such as in the back of a car or in a meeting room, restaurants, bistros, coffeeshop, hotel lobby or etc. Staff must lock the screen or log off when the device is unattended.
- 2.7 Staff may choose to register the use of their own personal device to setup corporate accounts; however, the staff must comply with all applicable policies, standards and guidelines set forth by the company. (See section BYOD)
- 2.8 Staff can access, use, or share the company proprietary information only to the extent it is authorized and necessary to fulfil their assigned job duties.
- 2.9 Staff must report virus or security warnings to Group IT service desk and avoid causing an alarm to others unnecessarily by forwarding or distributing virus warnings/alerts around.
- 2.10 Where possible, Staff must secure their devices so that all the data on it is encrypted and only accessible if the password is known.
- 2.11 Staff are not allowed to take their own personal backups of the company's data in any form, this includes physical or cloud storage.
- 2.12 System level and user level passwords must comply with Group IT defined password standards.
- 2.13 Staff must ensure that their assigned device(s) is protected from physical damage and is not exposed to situations in which it may become damaged.

ITP0201 Acceptable Use Policy (AUP)

- 2.14 All mobile and computing devices that connect to the internal network must comply with the company's security requirements.
- 2.15 All computer assets, services, hardware, or software to be used by the Staff within the company must be purchased through the Group IT or the appointed regional IT partners. For other personal computing assets, please refer to BYOD section.
- 2.16 Faults with the company's assigned device must be logged with the Group IT's Service Desk and repaired by the company's appointed vendors. Staff cannot engage or attempt to repair the devices by themselves or by unauthorized vendor.
- 2.17 Staff except authorized individuals must not remove any identifying marks on the company's device such as a company asset tag or serial number.
- 2.18 All personal, vendors or third parties owned device(s), including peripheral storage device(s) must be assessed by Group IT Security for their security adequacy before it is allowed to connect to the company's office network. Access granted must be based on need-to-basis and limited period.
- 2.19 The organisation will take steps to block the following categories but not limited to the following types of websites:
- Pornographic.
 - Violence.
 - Hate and discrimination.
 - Hacking.
 - Web chat.
 - Gambling.
 - Dating.
 - Radio stations.
 - Games.
 - Media Streaming.
- 2.20 For vendors or third parties who are given login access to the company's IT resources as part of their services in their support agreement; department or company's personnel who is managing this relationship must ensure they are aware of the company's Acceptable Use Policy (AUP) through the contractual supplier agreement and/or non-disclosure agreement.
- 2.21 All employees with information system access must undergo Group IT's or associated department's Cybersecurity awareness training as arranged.

Software Use

- 2.22 All installed software programs will be registered in the name of the company, not the individual. All purchased software is a corporate asset and licenses will frequently be reused as the shape of the company changes. Under no circumstances will corporate software be copied (other than for backups) or installed for use on non-corporate machines, such as at home. This is against the law.

ITP0201 Acceptable Use Policy (AUP)

- 2.23 Only software that is endorsed by the Group IT can be installed onto the company's computing devices (i.e., Laptop, desktop or mobile). Non-endorsed software will require explicit approval from the staff's supervisor and Group IT security team prior to installation. Such software will also have very limited support from Group IT.
- 2.24 Staff are responsible for exercising good judgment regarding the reasonableness of personal use. In the absence of such guidelines, Staff should be guided by company policies on personal use, and if there is any uncertainty, Staff should consult their supervisor or manager.
- 2.25 Staff are expected to understand and comply with the Copyright laws and regulations to legally protect the company and its associated companies or brands locally or globally.

Email Use

- 2.26 Staff must exercise vigilance when opening e-mail attachments, which may contain malware.
- 2.27 Staff must use the company's corporate email system for conducting business. All emails sent from the company's systems are in the possession and control of the company and are monitored for inappropriate use.
- 2.28 Staff cannot email with information classified as confidential or above (in accordance to the company's data classification) to external recipients without written approval from their supervisor or Manager. Where approval is not possible, Staff must at least have their supervisor copied in the email for their awareness. Email with such information must also be encrypted before sending.
- 2.29 Information classified as confidential or above (according to the company's data classification) can be emailed unencrypted internally on a need-to-know basis.
- 2.30 All incoming and outgoing emails must be managed via content protection that provides filtering, anti-spam and malware protection.
- 2.31 Postings by Staff from the company's email address to newsgroups or discussion forums must contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the company, unless posting is required for business purpose and approved by the supervisor.

Social Media and Blogging

- 2.32 Appropriate use of social media websites must be followed by Staff as they are legally liable for anything written or presented online. Staff must exercise sound judgement and common sense if posting articles, sharing of information or comments regarding the company.
- 2.33 Staff must express ideas and opinions in a respectful manner and never represent themselves or the company in a false or misleading way.
- 2.34 Blogs and social media platforms hosted on the company's owned domains or social media websites must be used in a way that adds value to and promotes business to the company.
- 2.35 Staff must not disclose any classified information about the company without written approval from their supervisor or manager.
- 2.36 Staff must ensure that there are no inappropriate links, updates, photos, video and other content on the postings or commentary made about the company.
- 2.37 Staff must respect the privacy and sensitivity of the company's Staff and customers, who reflect a diverse set of customs, values, and points of view. Ethnic slurs, personal insults, obscenity, etc. must not be written or commented on websites.

Online collaboration services (e.g. O365, Sharepoint, MS-Teams, etc.)

- 2.38 Sensitive data must not be downloaded from online collaboration services and stored on mobile devices unless it is absolutely necessary. If sensitive data is stored on a mobile device, it must be appropriately secured through encryption.
- 2.39 Mobile Device Management (MDM) or Mobile Application Management (MAM) is to be managed through Group IT Security Team's authorized management tools.

Bring your own device (BYOD)

- 2.40 The owner of the personal device is responsible for maintaining the device security, regular software updates and implementing security controls (i.e Anti-malware, software firewall, mobile protection, etc.).
- 2.41 The owner of the personal device must ensure backup is performed regularly to prevent data loss through security breach or device malfunction.

ITP0201 Acceptable Use Policy (AUP)

- 2.42 The staff acknowledge that he/she understood the risks involved and agree to hold the company harmless in case of any data loss or security breach on their own personal device.
- 2.43 In the event of staff termination or resignation, the company holds the right to remotely wipe all corporate data from their registered personal device(s).
- 2.44 Group IT will not be responsible for ensuring that company's implemented controls / managed applications will be or remain interoperable with the owner's personal device. In short, Group IT will not be responsible to troubleshoot the staff registered personal devices.
- 2.45 The company reserves the right to remove or wipe corporate data from the staff's registered personal device without prior notice in the event of security breach or policy violation. This action cannot be used against the company in any legal action(s).
- 2.46 The company reserves the right to monitor the staff's registered personal device activity and access corporate data stored on your device for security compliance or investigative purposes. This action cannot be used against the company in any legal action(s).

Audit and Inspection

- 2.47 For security and system/network maintenance purposes, authorized individuals within the company may monitor equipment, systems, and network traffic at any time.
- 2.48 In the event when the company suspects potential security compromise, it reserves the right to restrict the access to the device and/or ask the Staff to return the device to the Group IT service desk for inspection and audit.
- 2.49 In order to ensure its data is adequately protected, the Group IT reserves the right to be able to monitor and audit the device to ensure it meets the level of compliance with this policy. The level of monitoring and audit will be appropriate to the classification of the information held on the device.

3 Unacceptable Use

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into these examples of unacceptable use.

The following activities are strictly **PROHIBITED**, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the company.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the company or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server, or an account for any purpose other than conducting the company's business, even if Staff have authorized access, is prohibited.
4. Introduction of malicious programs into the network, computers, or servers (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing account password to others or allowing use of account by others is prohibited. This includes family and other household members when work is being done at home.
6. Writing down or disclose any password or authentication code that is used to access company information, assets or Critical Facilities is prohibited.
7. Using the company's computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any of the company's account or network.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which each Staff is not an intended recipient or logging into a server or account that the Staff is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless approved from Group IT Security team.
11. Executing any form of network monitoring which will intercept data not intended for the Staff 's host unless this activity is a part of the Staff 's authorised job/duty.

ITP0201 Acceptable Use Policy (AUP)

12. Circumventing user authentication or security of any host, network, or account.
13. Interfering with or denying service to any user other than the Staff's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about or lists of the company's staff to external parties without approval.
16. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals or other organisation or who did not specifically request such material (email spam).
17. Sending any form of harassment via email, telephone or other means of communication, whether through language, frequency, or size of messages. Types of harassment include but not limited to the following:
 - a. Message that can be deemed to convey abusive, threatening or bullying to recipient.
 - b. Message context either discriminates or encourages discrimination on the grounds of race, gender, sexual orientation, marital status, disability, political or religious beliefs.
18. Unauthorized use, or forging, of email header information.
19. Use of email auto-forwarding to personal or individual email address. as there is a possibility that this can result in classified information being forwarded to a recipient's email that does not have sufficient security clearance for the level of information involved. Furthermore, phishing and malware infected emails can get propagated or distributed to other unknowing staff.
20. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
21. Posting the same or similar non-business-related messages to large numbers of recipients.
22. Downloading data or programs of any nature from unknown/unsolicited sources.
23. Staff are prohibited from revealing any non-public or proprietary information, trade secrets or any other material covered by the company's data classifications to any unauthorised entity or on the internet.
24. Staff shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of the company and/or any of its employees. Staff are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging.
25. Downloading or forwarding office email or informational asset belonging to the company to personal email (e.g., Hotmail, Gmail, Yahoo, etc.) or personal cloud storage is strictly prohibited.

ITP0201 Acceptable Use Policy (AUP)

- 26. Sharing or transmission of company or third-party data through the use of personal email accounts is strictly prohibited.
- 27. Use of company assets and resources to perform crypto mining is strictly prohibited.
- 28. Knowingly transmit of malware infected data or phishing emails to others.
- 29. Sharing of account with other individuals other than yourself is prohibited.
- 30. Under no circumstances can any staff be allowed to bring in their own networking devices including Wireless Access Point, personal computing devices and connect into the company's network without explicit approval from Group IT.

4 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.

5 Reporting for Violations

Any violation of this Policy 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 Policy document may be subject to disciplinary action, including dismissal and legal action.

This page is intentionally left blank.