



KUOK (SINGAPORE) LIMITED

Information Security Policy

Classification	INTERNAL
Document Reference	ITP0101
Document Version	2.3
Document Status	FINAL

Revision History

Version	Date	Summary of Changes
1.0	28 Dec 2018	First copy
1.1	29 Apr 2019	Added "Replaced Policy" section
2.0	02 Mar 2020	Change of Approver
2.1	19 Nov 2020	Change of Approver
2.2	22 Mar 2023	Updated "General" section
2.3	28 Aug 2023	Renamed policy name ISMS11001 to ITP0101 and revised policy contents.

Authors

Name	Title
Jonathan Ong	Senior Manager, IT Security
Foo Tze Uei	Manager, IT GRC

Approval

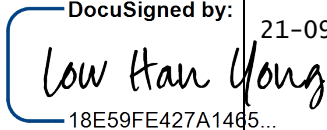
Name	Position	Signature	Date
Low Han Yong	CIO, Group IT	<div>DocuSigned by:  18E59FE427A1465...</div>	21-09-2023

Table of Contents

1	Introduction.....	6
2	Objectives.....	6
3	Acceptable Use.....	7
4	IT Risk Management	7
4.1	IT Risk Management.....	7
5	Computer Security	8
5.1	Equipment Protection	8
5.2	Equipment Maintenance.....	8
5.3	Security of Off-Premises Equipment	8
5.4	Security of System Files.....	9
6	Network Security	10
6.1	Network Security Design	10
6.2	Network Security Implementation.....	10
6.3	Network Security Configuration.....	10
6.4	Network Access Control	11
6.5	Intrusion Detection and Prevention (IDS/IPS).....	11
6.6	Wireless Network Security	12
6.7	Penetration Tests.....	12
7	Anti-Virus and Anti-Malware	13
8	Information Classification.....	14
8.1	Information Classification.....	14
8.2	Information Labelling	15
8.3	Information Handling	15
8.4	Periodic Review	15
9	IT Asset Management	17
9.1	Inventory of IT Assets.....	17
9.2	IT Asset Reporting and Lifecycle Management	19
9.3	Physical Asset Disposal	20
10	Access Control	21
10.1	Access Control Management	21
10.2	User Account Management.....	21
10.3	Default Password.....	22
10.4	Password Use	23
10.5	Password Maintenance.....	23
10.6	Account Locking.....	23
10.7	Network Access	23
11	Data Encryption	25
11.1	Risk Management	25
11.2	Encryption Techniques	25
11.3	Key Management.....	25

12	Data Backup	26
12.1	Backup Strategy	26
12.2	Backup Planning	26
12.3	Backup Schedule and Frequency	26
12.4	Backup Media Classification	27
12.5	Security Controls	27
12.6	Backup Media Inventory	27
12.7	Data Restoration Process	27
12.8	Backup Media Destruction	27
13	Data Retention and Disposal	28
13.1	Responsibilities	28
13.2	Retention and Disposal Requirements	28
13.3	Disposal Process	28
13.4	Periodic Review	29
14	Media Handling	30
14.1	Removable Media Management	30
14.2	Media Disposal	30
15	Vulnerability and Patch Management	31
15.1	Roles and Responsibilities	31
15.2	Vulnerability Monitoring	31
15.3	Vulnerability Scanning	32
15.4	Vulnerabilities Remediation	32
16	IT Incident Management	33
16.1	IT Incident Management Process	33
16.2	Roles and Responsibilities	33
16.3	IT Incident Record	34
16.4	IT Incident Tracking and Monitoring	34
16.5	IT Incident Classification	34
16.6	IT Incident Prioritization	35
16.7	IT Incident Escalation	35
16.8	IT Incident Response Team	35
16.9	Security Incident Response	36
17	IT Disaster Recovery	39
17.1	IT Disaster Recovery Plan	39
17.2	Testing and Monitoring	39
17.3	Third Parties or Service Providers	39
18	Logging and Monitoring	40
18.1	Time Synchronization	40
18.2	Audit Logging	40
18.3	Log Review	40
18.4	Log Monitoring	41
18.5	Audit Log Protection	41
19	Security Awareness Training	42

19.1 Cyber Awareness Training42

19.2 Cyber Phishing Simulation42

20. Deviation from Policy.....43

21. Reporting for Violations43

22. Disciplinary Actions.....43

1 Introduction

This section provides an overview of the policy, its purpose, and scope. It may also include a statement about the organization's commitment to information security.

Information Security is everybody's responsibility.

Kuok Singapore Limited (KSL) and its group of companies and subsidiaries hereinafter referred to as KSL.

KSL information systems are provided for business use only.

Use of any KSL information system for personal reasons (including e- mail and the web) is only permitted in accordance with the guidance in this policy.

KSL Group IT reserves the right to monitor any aspect of its information systems in order to protect its lawful business interests. Information gathered from such monitoring may be used to instigate or support disciplinary proceedings.

Breach of this policy will result in disciplinary action or penalty. Depending on the severity of the breach, this may include: -

- An informal warning from immediate manager
- A formal verbal or written warning for misconduct
- Dismissal for gross misconduct
- Termination of working partnership
- Criminal proceedings
- Civil proceedings to recover damages

2 Objectives

The main objectives of the policy are about safeguarding information assets, protecting against unauthorized access, ensuring compliance with applicable laws and regulations, and promoting a security-conscious culture.

3 Acceptable Use

This section establishes guidelines for the appropriate use of information systems, networks, and resources within the organization. It outlines acceptable behaviors, restrictions, and prohibited activities, such as unauthorized access, data breaches, and misuse of resources.

- For detailed information, please refer to the company's published *Acceptable Use Policy*.

4 IT Risk Management

The purpose of this section is to ensure a formalized approach to Information Technology (IT) Risk Management which encompasses key steps in identifying and managing risks in line with business needs and objectives.

Risk Management allows for determining areas of vulnerabilities; understand corresponding threats and identifying key risks through a Risk Assessment process. It also leads to selecting, implementing, and testing safeguards or controls to treat or minimize the impact of risks.

4.1 IT Risk Management

- a) Group IT to define the IT Risk Management framework that enables the review of IT risks.
- b) Group IT to establish the review frequency and key stakeholders from each domain (Application, Infrastructure/Network, Security)
- c) Group IT to establish the risk register where all discussed risks are recorded.

5 Computer Security

Computers (namely desktops and laptops) are a key area of security vulnerability for any organization. This section defines the security principles that apply to all company computers. These principles cover physical, network and system security for desktops and laptops, and should be used in conjunction with those other policy documents identified.

5.1 Equipment Protection

The following standards **MUST** be applied to protect physical access to computers:

- a) Any location within the offices or premises in which the company computers are located **MUST** be secure and **MUST** prohibit unnecessary access to work areas by unauthorized personnel.
- b) IT **MUST** isolate or secure computers requiring special protection in order to lower the general level of protection required in an area for other devices where not deemed required.
- c) Measures **MUST** be adopted to minimize the risk of potential physical threats to computers, including theft, destruction, or alteration of the asset.
- d) All employees **MUST NOT** eat, drink, or smoke near the computers in a computer room or data center.
- e) Environmental conditions which may damage the operation of computers, such as temperature, exposure to liquids and humidity, **MUST** be monitored.

5.2 Equipment Maintenance

- a) A qualified engineer **MUST** be engaged to perform repairs and troubleshooting of computers as required.
- b) When troubleshooting equipment or devices with sensitive information, the owner or authorized personnel **MUST** be present during troubleshooting.
- c) The manufacturer's instructions or recommendation to protect the equipment, including the protection against electromagnetic fields, **MUST** be respected at all times.

5.3 Security of Off-Premises Equipment

- a) Computers used out of the premises **MUST NOT** be left unattended in a public space or in areas (e.g. Vehicles, bags) where it could lead to harm or theft.
- b) Laptops and Tablets **MUST** be carried as hand luggage.
- c) User **MUST** take precautionary measures where confidential or sensitive information is used or transferred when working from home or while travelling. Some sample precautionary measures examples:
 - Encrypt such data before sending;
 - Scan all attachments before opening;
 - Avoid storing such data in personal devices or storage media (e.g. USB, Ext. Drive, Cloud storage, etc).

ITP0101 Information Security Policy

- d) Access control to computers and secure communications **MUST** then be applied where deemed appropriate.

5.4 Security of System Files

- a) The update of software, applications and libraries **MUST** only be performed by authorized personnel or party.
- b) Systems **MUST** contain only authorized software and applications.
- c) Systems **MUST NOT** contain any components that are end of life or without maintenance support from the vendors.
- d) A software lifecycle strategy **MUST** be implemented to ensure system integrity.

6 Network Security

The purpose of this section is to provide requirements for network security, particularly firewall design and implementation, access control and intrusion prevention.

6.1 Network Security Design

- a) Network documentation **MUST** be created, maintained, and be subjected to a review and approval annually or upon major changes to network architecture.
- b) All network changes **MUST** be risk assessed through change management process prior to implementation.
- c) All responsibilities for logical management of the network devices **MUST** be documented and kept up to date.
- d) All logical management of devices including the organizations (groups), individual roles within the organizations and responsible resources for each task **MUST** be defined.

6.2 Network Security Implementation

- a) All connections from external network segments i.e., internet or extranet, to internal network segments **MUST** go through demilitarized zone (DMZ) or firewall.
- b) All outbound connections from internal network segments **MUST** go through a Firewall. Any changes to existing connections must be managed through the company's change management process.
- c) Servers and non-end user devices **MUST NOT** be allowed Internet access, except to approved sites.
- d) All internal network information **MUST** not be disclosed to external networks.
- e) Firewall rule base reviews **MUST** be performed at least every six months. Each review **MUST** be recorded, and corrective actions **MUST** be conducted if necessary following change management process.
- f) The implementation of any new networking devices (i.e., routers, switches, firewalls, wireless access point, etc.) **MUST** follow the Group IT change management process and be approved by IT Management.
- g) Any wireless network for guest or visitor use **MUST** be validated by IT before being implemented and **MUST** be segregated from and **MUST NOT** have direct access to the company's internal network.
- h) Wireless access **MUST** be authenticated and encrypted based on the company's prescribed standards.

6.3 Network Security Configuration

- a) All non-essential and non-secure services on network devices **MUST** be disabled.
- b) Any enabled service **MUST** be restricted to specific ports between specific hosts and **MUST** be documented.

ITP0101 Information Security Policy

- c) All non-approved inbound or outbound traffic **MUST** be explicitly denied in the firewall rules or router access lists (ACL).
- d) Logging **MUST** be enabled for all firewall policies.
- e) Network devices **MUST** log relevant activity as described in IT Logging and Monitoring.
- f) The monitoring of equipment, systems and network traffic **MUST** only be performed by authorized individuals for security and network maintenance purposes.
- g) Network devices **MUST** be reviewed periodically to verify configuration. The use of an automated tool may be used in place of manual reviews.
- h) All configuration standards **MUST** be reviewed annually.
- i) Stateful inspection i.e., dynamic packet filtering **MUST** be enabled in the systems supporting it.
- j) In the network edge address spoofing detection **MUST** be enabled to prevent internal address ranges entering from external network interfaces.

6.4 Network Access Control

- a) Any information on network devices **MUST** be restricted to authorized users only in accordance with the IT Information Classification Policy.
- b) IT **MUST** implement a level of controls on all network connections based on the type and purpose of the connection that are sufficient in protecting the company's information and systems.
- c) Traffic from the Internet into any company networks **MUST** be denied by default. Required access **MUST** be explicitly allowed and be in accordance with IT Access Control Policy.
- d) A network access whitelist **MUST** be maintained and reviewed at least annually.

6.5 Intrusion Detection and Prevention (IDS/IPS)

- a) A Risk Assessment exercise **MUST** be conducted which will dictate where IDS/IPS is implemented on the Network.
- b) IDS and/or IPS **MUST** be used to monitor all traffic at the perimeter as well as network segments.
- c) Results from the intrusion detection system, above a pre-defined threshold, **MUST** be identified and **MUST** alert personnel of suspected compromises.
- d) All intrusion detection and prevention engines, baselines, and signatures **MUST** be kept up to date.

6.6 Wireless Network Security

- a) A process must be implemented to identify and deny unauthorized wireless access or attempts to connect to the company's wireless network.
- b) If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), monitoring MUST be configured to generate alerts to IT support personnel.
- c) Any unauthorized attempt to access to the company's wireless network will be investigated.

6.7 Penetration Tests

- a) External facing network penetration tests (cloud based application/services optional) MUST be conducted at least annually and after any significant infrastructure or application changes.
- b) Following a penetration test, after vulnerabilities have been addressed, another penetration test MUST be conducted to confirm remediation has been effective.
- c) Penetration tests for external facing network MUST be conducted by a qualified company.

7 Anti-Virus and Anti-Malware

- a) All computers whether connected to the company's network or standalone, MUST use approved anti-virus and anti-malware software and configuration.
- b) The anti-virus and anti-malware software MUST not be disabled or bypassed.
- c) The settings for the anti-virus and anti-malware software MUST not be altered in a manner that will reduce the effectiveness of the software.
- d) The automatic update frequency of the anti-virus and anti-malware software MUST not be altered to reduce the frequency of updates.
- e) All servers attached to the network MUST utilize approved anti-virus and anti-malware software.
- f) Every virus/malware infection in the company's environment or has indirect impact to the company (e.g. BYOD infected devices with company's data) constitutes a security incident and must be reported to Group IT Security as soon as possible.
- g) If email gateway is deployed in the company's IT environment, then it MUST be protected by approved email anti-malware software and hardened appropriately.

8 Information Classification

The purpose of this section is to describe the classification scheme used to categorize information based on its sensitivity or criticality. It outlines the requirements and handling procedures for each classification level, including access controls, storage, transmission, and disposal.

8.1 Information Classification

- a) The Information Owner is responsible for the appropriate classification of the information under their ownership which is originated from their department or received in first instance from external parties. The Information Owner **MUST** be departmental head who has a vested interest in ensuring the information is accurately and appropriately secured.
- b) The Information Owner is responsible for ensuring the availability of protective measures for safeguarding the classified information under their ownership.
- c) When classifying information, Information Owners **MUST** use one of the following four categories to determine their classification:

Data Classification	Assessment Criteria						Examples
	Is it publicly available?	Distribution Group	Impacts individuals?	Impacts customers?	Financial Loss?	Regulatory penalties or litigation?	
• Level 0 - Public (or unclassified)	Yes	External	No	No	No	No	Marketing materials; job description; etc.
• Level 1 - Internal	No	Internal	No	No	No	No	Internally circulated content or emails. Policies, procedure, etc.
• Level 2 - Confidential	No	Internal	Yes	No	Possible	Possible	Personal details (i.e. NRIC, account details, medical details, birth certificate); payslip; VA Pen-test report; Audit report; etc.; Pricings.
• Level 3 - Sensitive	No	Internal	Possible	Yes	Yes	Possible	M&A contracts; trade secrets; intellectual properties; etc.

- d) Each department **MUST** maintain their own inventory list of informational asset types and the corresponding classification. The list **MUST** be reviewed and updated at least once a year.
- e) The Information Owner **MUST** communicate the information classification to the recipient when information is released from their custody.
- f) Information owner's approval must be sought for any content modification or access changes to their information, rated confidential and above.
- g) Information recipients who are in doubt of the classification of the information **MUST** ask their superior/manager to review the appropriate level of classification or may refer to the Information Owners.
- h) By default, if the classification of specific information is unknown then the information

classification is assumed to be at the level of “Internal.”

- i) Any information belonging to customer or about a customer that may contain Personally Identifiable Information (PII) and MUST therefore be treated as “Confidential” minimally. The same principle MUST apply to employee or staff of company.
- j) The Information Owner MUST reclassify information to a lesser classification if it is no longer sensitive and to a higher classification if it has become more sensitive.

8.2 Information Labelling

- a) Custodians are responsible for overseeing and implementing the necessary protection of information assets at the level classified by the Information Owner.
- b) All hard copy and electronic documents MUST be labelled by the Information Creator/Originator with the classification of the most sensitive information in them.
- c) For each classification level, handling procedures MUST be implemented by the Custodian covering storage, transmission, and destruction.

8.3 Information Handling

- a) Employees who have access to information other than Public is prohibited from sharing with any unauthorized individual. The sender MUST ensure that information is available to employees only on a “need to know” basis.
- b) Confidential or Sensitive information MUST be protected. All physical copies must be stored in locked cabinets or safes when not attended; electronic copies must be encrypted or stored in folders only accessible to authorised staff.
- c) If a copy of Confidential or Sensitive information needs to be destroyed the following process MUST be followed:
 - Paper copies MUST be shredded using a cross-cut shredder.
 - Encrypted copies on any type of media, or copies on fully encrypted media, MUST be deleted.
 - Unencrypted copies on non-reusable electronic media MUST be physically destroyed.
 - Unencrypted copies on re-writable magnetic or optical media MUST be securely deleted.
 - Unencrypted copies on solid-state electronic media MUST be deleted.
- d) Use of any encryption solutions MUST be approved by Group IT Security. When approved solutions are used, standards for password strength, key-length and other parameters, key management, etc, MUST also be followed.
- e) All removable media containing classified information MUST be approved by the department head.

8.4 Periodic Review

- a) Information Owners MUST review the classification of information annually to determine if the classification needs change.

ITP0101 Information Security Policy

- b) Information Owners **MUST** also review the classification of information at any other time there is a significant change of circumstance that might alter the sensitivity of information, such as a change in legal requirements or a change in the usage of the information.
- c) If there is any change in classification, the Information Owner **MUST** perform the following:
 - Notify any change in classification of the information to the concerned Information Custodian(s).
 - Notify any change in classification of the information to the affected recipient(s) and remind recipients of handling requirements.
 - Update the information asset inventory.

9 IT Asset Management

The purpose of this section is to provide details for IT Asset Management (ITAM). The document outlines methods used to create and manage asset inventories, create ownership, a culture of asset accountability and enhance asset cost performance through asset lifecycle management. This policy document provides requirements for ownership and control of IT hardware and software assets.

9.1 Inventory of IT Assets

- a) IT MUST define an approved catalogue of IT equipment that can be officially purchased by the company. This MUST be periodically reviewed and kept up to date with technology changes that will benefit the company.
- b) Any new asset that is available on the catalogue MUST be acquired by Group IT.
- c) Any exception to asset acquisition MUST be documented by the Asset Owner and validated by Group IT.
- d) IT MUST create and own an Asset Inventory of all IT assets (hardware and software) for which they are responsible.
- e) Each IT asset MUST be identified and documented within the Asset Inventory. The assets could be in the form of:
 - All IT hardware including but not limited to servers, monitors, notebooks, tablets, smart phones, removable storage etc.
 - All IT software and license information.
- f) The IT Hardware Asset Inventory MUST include a listing of at least the following information for each asset:
 - Asset name
 - Serial number
 - Manufacturer
 - Model number
 - Asset type
 - Asset owner
 - Site location
 - Purchase date or lease contract commencement
 - End of support or end of life date (if available)
 - Warranty expiry date
 - Configuration (e.g, OS, version etc)
 - Asset status (e.g., In use, Spare, Written Off)
- g) Software asset information MUST be stored in an asset inventory and MUST include the following information:
 - Software name

ITP0101 Information Security Policy

- Vendor/ Supplier information
 - Version
 - License number
 - Type of license (single/corporate etc)
 - Device where installed (asset number) (if applicable)
 - Purchase date (if applicable)
 - End of support information (if available)
- h) The Asset inventory MUST be updated on a regular basis and an annual global review MUST be performed.
- i) IT staff who is responsible for asset management MUST:
- Verify that all hardware and software IT assets are logged in the IT asset inventory.
 - Verify that IT asset inventory is up to date – conduct at least annual inventory audits for hardware and software.
 - Reconcile installed software with owned licenses scheduled and officially implemented on an annual basis.
 - Work with software vendors in true-up of license counts when applicable.
 - Ensure local regulations and laws are being followed regarding use of software licenses.
 - Ensure that IT assets are managed in accordance with the lifecycle – for example end of support items are upgraded as required.
 - Ensure all hardware assets are identified and labelled with asset tags. This information MUST correspond to entries in the Asset Inventory.
 - Ensure that IT Asset Inventory is reviewed and updated at least every 6 months by the IT asset owners.
 - Enforce the process, where assets cannot be located it MUST be reported IT asset owner for investigation.
 - Ensure processes are in place to annually review assets with IT Security to assess systems for security vulnerabilities.
 - Ensure that hard copies of software license information, support agreements, warrantee information, etc. are stored in a secure storage location. This information MUST be stored in an organized format with easy access for the Asset Manager and available for asset owners.
 - Ensure that all items being used by the business have been properly acquired. All items in use by the business and not in the Asset Inventory system MUST be addressed.

ITP0101 Information Security Policy

- j) Procedures for asset labelling and handling **MUST** be developed, implemented, and maintained.
- k) The Asset Inventory system **MUST** be updated to reflect changes within 30 days of the change.
- l) Asset transfer between different business departments within the company **MUST** implement the following:
 - Ownership transfer within asset register. All relevant information fields within the asset register(s) **MUST** be updated to reflect the change of ownership of an asset.
 - Maintenance and licensing agreements (and costs) are transferred.
 - Any residual data **MUST** be removed to ensure that no residual data is moved and available to parties that would not otherwise have access.
 - Any residual data that must be available for the transferee must be duly approved and agreed upon between the involved departmental heads.

9.2 IT Asset Reporting and Lifecycle Management

- a) Asset acquisition **MUST** have prior written approval from Group IT.
- b) Asset reports using information from the Asset Inventory **MUST** be established and distributed to asset owners on an annual basis.
- c) End of Life and End of Support timeframes **MUST** be tracked within the Asset Inventory system to assist asset owners with lifecycle management.
- d) A maintenance contract level **MUST** be defined based on the risk assessment and cost benefit analysis for any asset until end of life is reached.
- e) Any maintenance contract level **MUST** be reviewed annually based on the risk assessment for each asset and the maintenance contract **MUST** be renewed for each asset with respect to the requirements.
- f) Information regarding assets **MUST** be available to the business as required through the Asset Inventory to perform necessary ad hoc reporting and financial forecasting, such as capital replacements.
- g) During the life cycle of software assets, IT and Asset Owner **MUST** ensure:
 - When software items are received and deployed, all relevant information is logged in the Asset Register – for example license information and where application has been deployed.
 - Ongoing license, maintenance and support agreement management processes are observed through the life of the software. The requirements may differ across different applications.

- During the decommissioning phase, applications are removed from devices with all license, maintenance and support agreements ended as required.

9.3 Physical Asset Disposal

- a) IT Staff members **MUST NOT** be allowed to dispose of asset without a management approval.
- b) Before each asset is disposed of, component storing data **MUST** be removed. These components disposal **MUST** follow with the company's Disposal of Media procedure.
- c) Asset with storage component that cannot be removed **MUST** be securely erased in compliance with the IT Media Handling Policy before disposal and IT Information Classification Policy.
- d) The following options **MUST** be considered for assets identified for disposal:
 - i) Transfer to another department
 - ii) Private sale
 - iii) Destroyed or recycled
 - iv) Donations
- e) Selling an asset **MUST** be under control of financial department.

10 Access Control

The purpose of this section is to address the requirement for access control to information systems. It is focused on the prevention of unauthorized access and the need for authorized access in accordance with the requirements of the business. This document applies to all individuals granted access to information systems resources. Information systems resources include all communication network components, business application systems and any computing system provided to users for the purpose of achieving the tasks in their assigned roles.

10.1 Access Control Management

- a) Access shall be granted based on the principle of least privilege, which means that each program and user will be granted only sufficient privileges necessary to complete their tasks.
- b) Access to data classified as “Sensitive” or ‘Confidential’ shall be limited to authorized persons whose job responsibilities require it.
- c) Access control MUST be implemented on each system to ensure access is limited to only authorized personnel.
- d) Administrators MUST utilize “administrator accounts” which are separate from their “user accounts” when performing administrative tasks on the information systems.
- e) Group IT must ensure split control for all break-glass privileged access and such access must be password rotated at least annually.
- f) Role-based access control (RBAC) SHOULD be used to secure access to ALL applications or resources that are accessible from the Internet.
- g) Multi-factor authentication (MFA) MUST be enforced on all cloud service access, including web mail services, that are publicly accessible.
- h) All access to company network or computing resources MUST be password protected.
- i) Applications should be configured with Single Sign-On (SSO) to the corporate Active Directory.
- j) Partner agencies or 3rd party vendors must only be granted access to our company’s IT environment on a need-to basis and removed when access is no longer needed.

10.2 User Account Management

- a) Users MUST have a specific business or operational need to request access to any systems.
- b) Duties and areas of responsibility MUST be properly defined to allow the privileged user ID’s to only have the required access rights necessary to perform their job responsibilities.
- c) A formal user registration and de-registration procedure MUST be put in place for granting and revoking access to all information systems and services.
- d) The registration and de-registration procedures MUST be approved by the appropriate information system or service owner.

ITP0101 Information Security Policy

- e) System owners **MUST** have their users' accounts and access rights reviewed on a regular basis following formal procedures.
- f) To enable traceability and accountability of access to the IT systems and devices, all users **MUST** have a unique, unshared user account and password. Users **MUST NOT** share their individual passwords with others.
- g) Requests for account creation or changes **MUST NOT** be approved by the same person who requested the creation or the change unless the requestor/approver is the information, system, or service owner.
- h) IT **MUST** separate duties of individuals as necessary, to prevent malevolent activity without collusion. Privileged users like administrators **MUST** have separate administrator accounts which are separate from their normal user accounts. Use of privileged accounts to empower personal or other user accounts is strictly prohibited.
- i) AD user accounts that are inactive for more than 30 days will be disabled immediately. To re-enable the account, the user's supervisor shall raise a service request ticket to IT Service Desk.
- j) AD user accounts **MUST** be revoked or disabled by close of business on the next working day after an individual has resigned or terminated. This requirement **MUST** be included in termination procedures or checklist.
- k) Upon staff position change or transfer, all his/her access rights **MUST** be reviewed within one month by their reporting manager.
- l) Associated procedures **MUST** retain evidence of timely account deletion, deactivation/disablement, or modification.
- m) Activities conducted under privileged accounts **MUST** be logged and reviewed for irregularities for any associated or reported incident. Evidence of reviews **MUST** be maintained for such investigation.
- n) Access controls to the information **MUST** be set in accordance with the company's information classification guidelines. For sensitive information, procedures **MUST** be created by the information owner to request approval from Senior Management or executive board/committee before granting access.
- o) Administrators **MUST NOT** use their privileged accounts for conducting unrelated administration activities (e.g., Web surfing, media streaming, etc).
- p) Group, shared, or generic accounts **MUST NOT** be used, except for the following conditions.
 - If these accounts are used for administrative purposes, they **MUST** be managed under GROUP IT Privilege Access Management process.

10.3 Default Password

- a) Configuration standards and procedures for all equipment **MUST** include the need for default password change.
- b) Before being placed or installed on the network, all devices **MUST** be assessed, and **MUST** be confirmed that all default password and account settings have been changed.

10.4 Password Use

- a) All IT assets must be password protected.
- b) Users are responsible for ensuring that their individual password remains secret. Users **MUST** not share their password with others.
- c) Passwords **MUST** be set in adequacy with the value and sensitivity of the information assets being protected and, at a minimum, **MUST** comply with IT minimum password standard.
- d) A clear desk and clear screen policy **MUST** be adopted to reduce the risk of unauthorized access or damage to papers, media, and information processing facilities.
- e) Assign all users a unique ID before allowing them access to any resources.

10.5 Password Maintenance

- a) Users **MUST** follow good security practices in the selection and use of passwords.
- b) Temporary passwords **MUST** be unique to an individual and **MUST NOT** be easily derived.
- c) All passwords **MUST** be unreadable during transmission using robust protocols.
- d) Passwords **MUST** not be physically written down and stored anywhere near the user's workstation.
- e) Passwords **MUST** never be stored on computer systems in an unprotected form.
- f) Secure channel **MUST** be used to transmit passwords. Passwords in clear text using an insecure channel **MUST** be prohibited (such as http, telnet, or FTP).

10.6 Account Locking

- a) To prevent unauthorized disclosure of information and unauthorized system usage, users **MUST** ensure that proper access restrictions (i.e. Password screenlock) are in place before leaving equipment unattended.
- b) Inactive sessions **MUST** shut down after a defined period of inactivity.
- c) All terminal connections **MUST** be configured to timeout after a designated period of inactivity.
- d) Reconnection to the terminal or session **MUST** require the user to properly re-authenticate.

10.7 Network Access

- a) All employees and contractors shall be given network access in accordance with the access control procedures with least-privilege principle.
- b) All staff and contractors who have remote access to company networks **MUST** be authenticated using the VPN authentication mechanism, which **MUST** include Multi-Factor Authentication.

ITP0101 Information Security Policy

- c) Segregation of networks **MUST** be implemented to separate the production network from the development or testing networks.
- d) All ports, services, and similar facilities installed on a computer or network, which are not specifically required for business functionality, **MUST** be disabled or removed.

11 Data Encryption

The purpose of this section is to establish guidelines and procedures for the encryption of sensitive data to ensure its confidentiality and integrity. Encryption plays a crucial role in protecting data from unauthorized access, interception, or modification. This policy aims to safeguard KSL's data assets and comply with applicable privacy and security regulations.

11.1 Risk Management

- a) All data must be classified based on its level of sensitivity and the associated risk. Encryption requirements may vary depending on the classification level.
- b) Encryption at Rest: Sensitive and Confidential data stored on servers, databases, or any other storage media **MUST** be encrypted. This includes data at rest in physical and virtual environments.
- c) Encryption in Transit: Sensitive and Confidential data transmitted over wired and/or wireless networks **MUST** be encrypted using secure protocols. at rest and in transit using encryption algorithm approved by IT.

11.2 Encryption Techniques

- a) All encryption technologies and techniques used by KSL must be approved by Group IT Security.
- b) Refer to Group IT's encryption standards documentation.

11.3 Key Management

- a) Encryption keys **MUST** be protected from modification, loss, destruction, and unauthorized disclosure.
- b) Encryption keys **MUST** be properly managed throughout their lifecycle, which includes secure generation, storage, distribution, rotation, and revocation.
- c) Access to encrypted data **MUST** be restricted to authorized personnels or systems with appropriate privileges.
- d) Access to encryption keys **MUST** be protected and limited only to authorized personnels.
- e) Private asymmetric and symmetric keys shall only exist in the following secure forms:
 - i. As cleartext within the memory of a hardware-based encryption device.
 - ii. As ciphertext outside the memory of a hardware-based encryption device.
 - iii. As two or more key fragments either in cleartext or ciphertext, managed using dual control with split knowledge.

12 Data Backup

The purpose of this section is to provide a formalized approach to manage the backup activities inside its infrastructure in accordance with identified business needs and objectives. The Data Backup Policy allows the implementation of secure backup processes, management of the media, definition of retention periods for each type of data and the definition of processes for data restoration and media destruction.

12.1 Backup Strategy

- a) IT is responsible to backup critical system data and files identified by business management and application owners.
- b) Backup systems for each production system **MUST** meet the requirements of the service level agreement and Disaster Recovery Plan as defined by the business.
- c) The extent (such as full backup or incremental backup) and frequency of backups **MUST** be documented and followed in accordance with business requirements. The level of backup **MUST** be defined to include critical systems information, applications, and data necessary to recover the complete system in the event of a disaster.
- d) IT **MUST** monitor the backup activity on a periodic basis to ensure backup is successfully completed. Any deviation or exception **MUST** be logged, and such deviation or exception is to be resolved within the specified timelines.
- e) IT **MUST** create and maintain the inventory list of backup copies up to date.
- f) Programs, documentation, recovery plans, contingency plans, and computer-generated information **SHOULD** be backed-up before and after significant changes are made to production systems.
- g) At the workstation level (e.g., PCs, laptops, etc), **ALL** employees **MUST** avoid storing critical business information and data locally in their workstations to avoid data loss due to device damage, theft or malfunction. Employees are recommended to store critical business information and data on Sharepoint or IT assigned network storage.

12.2 Backup Planning

- a) All system must perform a backup at least daily or commensurate with their determined needs and criticality.
- b) Where possible, execute and run backups **OUTSIDE** of office hours.

12.3 Backup Schedule and Frequency

- a) IT **MUST** consider the following factors when deciding the backup frequency:
 - Volatility of information on the data
 - Static content (less frequent backups)
 - Dynamic content (more frequent backups)
 - Type of data to be backed up (e.g., system, application, log, or user data)
 - Amount of data to be backed up (network bandwidth may limit the frequency)
 - Available backup technologies, media and devices.

- Alignment to information owner's data retention and RPO requirements.

12.4 Backup Media Classification

- a) Backup media **MUST** be clearly and distinctly labelled.
- b) Records **MUST** be categorized into record types with details of retention periods and type of storage media.
- c) The system of storage and handling **MUST** maintain a system for clear identification of records in accordance with retention periods.
- d) Backup media classification **MUST** follow the IT Information Classification.

12.5 Security Controls

- a) Confidential data **MUST** be made unreadable anywhere it is stored (including on backup media, portable digital media, and in logs) by using IT approved encryption standard.
- b) Cryptographic keying material associated with encrypted archives or digital signatures **MUST** also be stored to enable decryption of records for the period of retention.
- c) Backup **MUST** be cycled to an offsite location for safe keeping.

12.6 Backup Media Inventory

- a) IT must perform a review on backup media inventory annually.
- b) Auditable evidence of physical annual media inventory **MUST** be kept.
- c) All media backups **MUST** be clearly labelled to allow for their identification.
- d) Any media backup found to be missing **MUST** be reported in line with the Incident Management process.

12.7 Data Restoration Process

- a) The interval of data restoration testing for backup media is performed at least quarterly.

12.8 Backup Media Destruction

- a) Prior to media disposal, all data on electronic media **MUST** be rendered unrecoverable via degaussing or physical destruction.
- b) All media destruction **MUST** be properly tracked, and auditable evidence must be kept.

13 Data Retention and Disposal

This section ensures the company has a formalized approach in retaining and disposing business information stored either as hardcopy or electronically. It relates to information created, used, and possessed by the company in accordance with applicable legal, regulatory, and business requirements.

13.1 Responsibilities

- a) The Information Owner **MUST** define a Retention Schedule for each information asset they own, along with its classification as defined in the IT Information Classification Policy.
- b) All employees **MUST** be aware of and comply with this policy and the Retention Schedule. In addition to the other employee obligations set forth in this policy:
 - Each employee is accountable for storing and disposing of hardcopies and electronic information in accordance with this policy and the Retention Schedule.
 - Each employee is responsible for identifying any original hardcopy or electronic information within their possession or control.
 - All employees **MUST** not destroy any hardcopy or original electronic information before the Retention Schedule supports its disposal.
 - Once the electronic information retention period has elapsed, the employee who is responsible for that electronic information **MUST** take steps to destroy it. If the hardcopy or electronic information is confidential or proprietary information, then it **MUST** be disposed securely.
- a) When an employee leaves the organization, that employee's immediate supervisor becomes responsible for the retention or disposal of all electronic information for which the departing employee had responsibility.

13.2 Retention and Disposal Requirements

- a) When the retention of an electronic information is addressed in a contract or agreement, the requirements **MUST** conform to the Retention Schedule.
- b) The retention period **MUST** not be less than what is required in the Retention Schedule.
- c) In the case of individual contracts or agreements which require the company to retain specific electronic information beyond the normal retention period identified in the Retention Schedule, the retention period for that information **MUST** be followed as per the contracts or agreements.
- d) All information **MUST** be removed from the company's systems when the retention period has elapsed using an approved disposal method documented in this policy.

13.3 Disposal Process

- a) All employees including but not limited to Business Department Managers, Information Owners or Information Custodians **MUST** securely delete, destroy, or dispose of the electronic information when the associated retention period has elapsed as per either:

ITP0101 Information Security Policy

- the Retention Schedule
 - or when the computing devices such as servers or storage devices containing the electronic information are no longer needed for legal, regulatory, or business reasons.
- b) Copies or drafts of electronic information **MUST** not be held for longer than the scheduled disposal date of the original information.
- c) When instruction is given by IT and the Legal Department to suspend routine electronic information disposal, all identified information **MUST** be held until such time as the hold is lifted. This also applies to the situation where the retention period listed in the Retention Schedule has elapsed. Once the hold is lifted then routine disposal resumes and the information that had its retention period elapse during the hold **MUST** be destroyed.
- d) Media or Hardcopy materials **MUST** be destroyed when no longer needed for business, compliance, or legal reasons as per the company's media disposal procedures.

13.4 Periodic Review

- a) The Information Owner **MUST** review the information Retention Schedule at least every two years.
- b) The Information Owner **MUST** review the information Retention Schedule to determine if the retention period needs to be changed in the event that there is a significant change of circumstances that might alter the sensitivity of data. Such an event can include but not be limited to:
- A change in legal requirement
 - A change in the usage of the information
 - The launch of new services to customers
 - A service end of life

14 Media Handling

The purpose of this section is to provide the company with a formalized approach to ensure that media is controlled and physically protected to prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities. It details policy related to media storage and disposal, media distribution control and removable media management to ensure confidentiality and integrity of the information contained on the media, minimizing risk to the business.

14.1 Removable Media Management

- a) Removable media **MUST** only be used by an employee who has an identified business need approved by the business/department head.
- b) IT is responsible for:
 - the definition of the cases where removable media can be used.
- c) All company employees requiring removable media storage **MUST** follow the relevant procurement process, which will require appropriate management approval defined and endorsed by IT.
- d) Each end user is responsible for the appropriate use and security of data stored on media.
- e) All company Confidential and Sensitive data **MUST** be **encrypted** before storage on removable media devices. Moving Confidential or Sensitive data to removable media **MUST** be done only with *clear business needs and management approval*. Information relating to data classification is found in IT Information Classification Policy.
- f) Backup (e.g. DASDs or Tapes) media **MUST NOT** be removed from the company's infrastructure or premises unless it is done through a defined and agreed process or with specific authorization from the System Owner. A record **MUST** be maintained of all removable media sent off-site, brought into, or received by the company. This record **MUST** also identify the data files involved.
- g) If a user leaves the company, then they **MUST** return the removable media device to IT for secure destruction or redistribution.

14.2 Media Disposal

- a) Company **MUST** physically destroy, delete, or overwrite media containing sensitive information according to the company's Information Classification Guidelines.
- b) Whichever IT storage assets and media that malfunctioned or deemed non-operative can be physically destroyed as secure deletion is not possible, such assets physically destroyed must be witnessed by the local IT staff.

15 Vulnerability and Patch Management

The purpose of this section is to address the requirement for vulnerability and patch management. These are security practices designed to proactively prevent the exploitation of IT vulnerabilities that exist within the company.

Patches are additional pieces of code developed to address problems in software. Patches enable additional functionality or address security flaws within a program. Vulnerabilities are flaws that can be exploited by a malicious user to gain access or greater privileges than they are authorized to have on a system. Not all vulnerabilities have related patches, thus administrators must be aware of security issues and provide solutions to mitigate potential exploitation.

15.1 Roles and Responsibilities

- a) IT Cybersecurity team has the primary role of facilitating the identification, assess and approval of patches within the IT Organization.
- b) IT Cybersecurity team members **MUST** include individuals with knowledge of vulnerability and patch management, as well as system administration, intrusion detection, and firewall management.
- c) IT Cybersecurity team **MUST** do pro-active monitoring on vulnerabilities, patches, and threats through security advisories and vulnerability information sources according to the approved list of software and hardware. Monitoring consists of more than simply checking security newsletters for the latest vulnerabilities and exploits; it also entails evaluating security information to determine its applicability within the company based upon the technology usage and any underlying compensating controls.
- d) IT Cybersecurity team **MUST** track the remediation of vulnerabilities within the company.
- e) IT Cybersecurity team **MUST** maintain regular communication with the following stakeholders that have authority on all Vulnerability and Patch Management matters:
 - IT Operations
 - Infrastructure.
 - Application and Data
 - Governance Risk and Compliance
 - IT Business Partners (To identify, assess and prioritize IT Projects)

15.2 Vulnerability Monitoring

- a) To provide accurate and timely identification of newly discovered security vulnerabilities, the following **MUST** be established:
 - A centralized patch management tool or service, which provides a list of applicable patches based on a set of approved releases from product publishers and vendors.
 - A vulnerability database or service to obtain information on all newly public vulnerabilities and suggested remediation or alternative options if patches unavailable from vendors.

ITP0101 Information Security Policy

- A third-party vulnerability service that highlights the most critical vulnerability (CERT) such lists will help on remediation prioritization whilst referring to international guidelines and standards.
- b) All IT employees **MUST** be made aware of their responsibility to report any information regarding security events. Refer to IT Incident Management Policy for further information on responding to IT security incidents.
- c) Action **MUST** be taken in response to the identification of potential technical vulnerabilities:
 - Once a potential technical vulnerability has been identified, Cybersecurity team **MUST** define the associated risks and then ensure action is taken. Such action may involve patching of vulnerable systems and/or applying other controls.

15.3 Vulnerability Scanning

- a) Vulnerability scans **MUST** be completed on all systems on a regular basis to ensure appropriate security levels are maintained.
- b) Vulnerability scan results **MUST** confirm that security measures (settings and patches) have been properly implemented.
- c) An internal network vulnerability scan **MUST** be performed monthly and after any significant change in the network.
- d) **MUST** establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.
- e) All external network facing IT assets must be scanned by the company's approved scanning tool.

15.4 Vulnerabilities Remediation

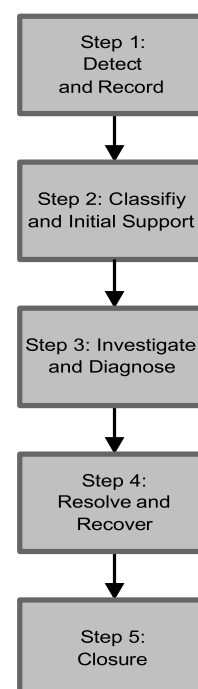
- a) The significance of the threat or vulnerability **MUST** be determined and evaluated on the impact on the company's systems if the vulnerability is not removed and may be exploited.
- b) The security architecture **MUST** be designed to automatically mitigate certain threats and reduce the urgency to apply patches.
- c) A vulnerability ranking based on CVSS (Common Vulnerability Scoring System) **MUST** be used to determine the vulnerability severity and this **MUST** measure the associated risk of the impacted resource with existing controls around, as that will provide a better risk assessment.
- d) The security assessment **MUST** be conducted by The IT Cybersecurity Team to ensure that all system components and software are protected from any known vulnerabilities by having the vendor-supplied security patches installed within one month of release. (Refer to company's prescribed patch standards)

16 IT Incident Management

The purpose of this section is to provide a formalized approach to govern the Incident Management process used to manage IT incidents. An Incident is an unplanned interruption or reduction of service that has an immediate or potential negative impact on the organization. The policy included reporting, investigation, containment, eradication, and recovery. It may also outline the escalation process and coordination with external parties (e.g., law enforcement, regulatory bodies) if necessary.

16.1 IT Incident Management Process

- a) IT Incident Management **MUST** have a clear relationship with IT Change Management Policy.
- b) IT Incident Management process **SHOULD** consist of several high-level activities:
 - **Step 1: Detect and Record**
An IT incident is detected, and an IT incident record is created.
 - **Step 2: Classify and Initial Support**
The IT incident is classified, and a priority is assigned. Initial support is given to identify if there is a quick fix to the IT incident.
 - **Step 3: Investigate and Diagnose**
The IT incident is investigated and diagnosed to identify the root cause.
 - **Step 4: Resolve and Recover**
Based on the identified root cause, a resolution is defined and implemented resulting in service recovery
 - **Step 5: Closure**
The service recovery is verified, the IT incident record is updated with resolution description and the incident record is closed.
- c) An assessment of the root cause **SHOULD** be completed under a post incident review to determine what preventative actions can be implemented to avoid a repeat of the same incident. Such preventative actions **MAY** include additional logging or additional triggers for certain alerts. This is only applicable for critical (P2) and emergency (P1) incidents.
- d) IT Incident Reporting **MUST** be distributed to stakeholders.



16.2 Roles and Responsibilities

- a) An Escalation matrix **MUST** be defined and outline which stakeholders **MUST** be informed, when and by whom.
- b) A directory with telephone and email contact details for Incident Notification **MUST** be available and kept current and accurate.

16.3 IT Incident Record

- a) All unplanned interruptions to or reduction in quality of an IT Service that has an immediate or potential negative impact on the organization **MUST** have an IT incident registered within the IT service management system/tool and be recorded, tracked, and monitored.
- b) Information that **SHOULD** be captured in the IT incident record includes:
 - A unique incident record number
 - Date and time of incident occurrence
 - Customer and contact information
 - Description of the incident
 - Classification (category and type)
 - Impact and urgency
 - Priority
 - Status
 - Assigned to (a group or person)
- c) IT Incident Management **MUST** facilitate continual improvement in all aspects including improvements to the IT Incident Management approach.
- d) All IT incident records **MUST** capture a resolution description prior to closure of the record.
- e) An incident record **MUST** be appropriately classified based on the type of incident.
- f) An incident **MUST** be managed according to service levels documented in the service level agreement (SLA).

16.4 IT Incident Tracking and Monitoring

- a) All incident records are tracked and monitored through the GROUP IT approved ITSM platform via the IT Incident Management process, from the opening of an incident record until the record is closed.
- b) Prior to closure of an IT incident record an activity log **SHOULD** be included in the record to capture time and actions performed. If the incident was solved with a work around then a Problem Record **SHOULD** be initiated for further investigation to identify a solution.

16.5 IT Incident Classification

- a) An incident **SHOULD** be classified by identifying a type and category and is used to assign a priority level.
- b) IT services **SHOULD** define the hierarchy and have their own SLAs. This hierarchy **SHOULD** be used to determine the impact:
 - IT Service (e.g., End User Computing)
 - System (e.g., Windows 10)
 - Component (e.g., Microsoft Office 365)
 - Item (e.g., Microsoft Word)
 - Module: (e.g., printer functionality)
- c) Prioritization of the IT incident **SHOULD** be set based on the business impact caused by the incident and the urgency to resolve (see the prioritization matrix). Therefore, classification is defined before prioritization of the IT incident.

16.6 IT Incident Prioritization

- a) An incident SHOULD be assigned a priority level (prioritization), based on business impact (High, Medium, Low) and urgency.

Priority	Impact	Urgency	Description
P1 Critical	High	High	Interruption making a critical functionality inaccessible causing a severe impact on services availability. There is no possible alternative.
	High	Medium	Critical functionality or network access interrupted, degraded or unusable, having a severe impact on services availability.
P2 Important	Medium	High	No acceptable alternative is possible.
	High	Low	Non-critical function or procedure, unusable or hard to use having an operational impact, but with no direct impact on services availability.
P3 Normal	Low	High	A workaround is available.
	Medium	Medium	Application or personal procedure unusable.
P4 Low	Medium	Low	A workaround is available, or a repair is possible.
	Low	Medium	

16.7 IT Incident Escalation

- a) For emergency IT incidents the IT incident response team MUST be assigned.
- b) If the emergency incident requires a change to be implemented for its resolution, then a Change Request MUST be classified as an emergency change and MUST be approved by an authorized person in accordance with IT Change Management Policy and Standards.
- c) Incidents that are not solved within agreed lead-times MUST be escalated.

16.8 IT Incident Response Team

- a) The IT Incident Response Team SHOULD be established to provide a quick, effective, and orderly response to IT incidents. It SHOULD be responsible for investigating suspected intrusion attempts or other security incidents in a timely, cost-effective manner and for reporting findings to management and the appropriate stakeholders as necessary.
- b) The Incident Response Team SHOULD be authorized to take appropriate steps deemed necessary to contain, mitigate or resolve an IT incident. The IT Incident Response Team is responsible for putting the IT Incident Response Plan into action.

- c) The IT Incident Response Team members MAY include roles such as:
- IT Operations Manager
 - IT Infrastructure Manager
 - IT Cybersecurity Manager
 - IT Governance Risk Compliance Manager
 - Application Teams
 - Participants from Business Departments
- d) The IT Incident Response Plan MUST be under document change control to ensure that the IT Incident Response Plan is adjusted and updated when changes in the environment or in the organization are made.
- e) Specific personnel MUST be designated and available on a 24/7 basis to respond to alerts.
- f) Evidence MUST be collected in conformance with the relevant rules of capturing forensically sound evidence (if any) as laid down by the law.
- g) All evidence collected and forensic examination tasks MUST be performed by a company appointed and trusted external third party.
- h) IT Incident Response Plan MUST address the following at minimum:
- Roles and responsibilities
 - Communication strategies
 - Reference or inclusion of incident response procedures from the payment brands
 - Specific incident response procedures
 - Business recovery and continuity procedures
 - Data back-up processes
 - Analysis of legal requirements for reporting data breaches
 - Coverage for all critical system components
 - Responses to all critical system components
- i) The incident response plan developed SHOULD be constantly reviewed to ensure that it reflects current requirements and reflects experienced gained within the organization.

16.9 Security Incident Response

- a) The following types of incidents SHOULD be reported to IT Incident Response Team:

Unauthorized Access
<ul style="list-style-type: none">• Report successful unauthorized access to [Company Name] systems (e.g., web site defacements, unauthorized root or administrator access).• Report unsuccessful unauthorized access attempts only if they are considered to be persistent (e.g., someone from the same source keeps locking out accounts trying to brute force passwords, an automated script keeps probing a [Company Name] web server causing response problems).• Report suspected unauthorized access, even if unproven, if you believe the incident MAY impact other [Company Name] entities.

Malicious Code
<ul style="list-style-type: none"> • Report instances of viruses, Trojans, worms, botnets, or other malicious code that have had widespread impact or adversely affected one or more mission critical servers at your site. • Report malicious code blocked by email proxies or other anti-virus software only if it seems to be persistent and beyond current Internet normal behaviors.
Denial of Service (DoS)
<ul style="list-style-type: none"> • Report all denial-of-service attacks that adversely affect or degrade access to critical services. • Report all other attempted denial of service attacks only if they are persistent or significant (e.g., attempted DoS attacks aimed specifically at your DNS servers or routers would be significant.)
Reconnaissance Scans and Probes
<ul style="list-style-type: none"> • Scans and probes that precede or are related to the incidents listed above SHOULD be reported as part of that incident. • Any other scans and probes SHOULD be reported only if they are persistent or significant.

Rapid Response

- b) The IT Incident Response Team MUST respond rapidly to all security incidents, liaising and coordinating with the company staff to gather information and offer advice.
- c) The IT Incident Response Team MUST conduct the following activities, but not be limited to:
 - Evaluating the current state of the system, extent of penetration or infection, type of data at risk and source or target of the attack.
 - Isolating and containing the threat in order to disengage the threat and identify as well as track the attack mechanism.
 - Overseeing recovery and restoration.
 - Beginning system remediation and identifying issues that may have contributed to the security breach.
 - Decide if local law enforcement authorities should be notified and notify these authorities if needed.

Documentation and Reporting

ITP0101 Information Security Policy

- d) All suspicious events related to suspected information security breaches, the company staff MUST formally report and provide the information to the IT Incident Response Team, or the company appointed external service provider.
- e) The IT Incident Response Team or the company appointed external service provider MUST forensically process, record and report the event.
- f) Company staff MUST maintain integrity of information and data during an investigation of information security incidents by employing dual control and segregation of duties as they relate to the nature of the investigation.

Qualified Personnel or Service Provider

- g) Only qualified and suitably trained IT Incident Response Team members or company appointed qualified third-party service providers can investigate all Information security incidents.

Information Release

- h) Only company authorized personnel is allowed to release information relating to an Information Security incident (internally and externally).
- i) If reporting is required by law or contractual obligations, company legal or communications department personnel MUST provide information regarding incidents that are required to be reported.

Periodic Test and Review

- j) IT Incident Response Team MUST review and test the IT Incident Response Plan at least annually and modify the plan according to lessons learned and/or incorporate industry developments.

Monitoring and Alerting

- k) IT Incident Response Team MUST ensure that information security incidents are being monitored on 24/7 basis and designated personnel are available to respond to alerts.

Training and Awareness

- l) Company management MUST provide appropriate training to staff with Incident Response responsibilities.

17 IT Disaster Recovery

This section defines the approach to managing IT Disaster Recovery for the most critical IT infrastructure and system.

17.1 IT Disaster Recovery Plan

- a) The Disaster Recovery plan MUST be:
 - Created and maintained for all critical IT system as identified and determined by the business during their Business Impact Assessment (BIA) process.
 - Distributed to all relevant staff to use in an emergency.
 - Kept up to date and subject to annual review exercise.
- b) The Disaster Recovery Plan MUST include:
 - Key infrastructure assets
 - Key contacts that can assist in the activation or recovery from disaster.
 - Defined scenario of what can be classified as a disaster.
 - Key communication plan of who to escalate or what to inform.

17.2 Testing and Monitoring

- a) Testing of Disaster Recovery Plan MUST be undertaken to ensure:
 - Contacts listed are reachable and valid.
 - Defined objectives are met.
 - Issues or shortcomings are identified and addressed.
 - Ensure all relevant staff familiarise themselves with Disaster Recovery process.
- b) Disaster Recovery Plans for critical IT resources or systems MUST undergo testing on an annual basis to ensure that the plans are valid and relevant.

17.3 Third Parties or Service Providers

- a) IT MUST assess third parties' Disaster Recovery capabilities when deciding on suitable providers. Third parties Service Level Agreements (SLAs) MUST reflect their Disaster Recovery policy/criteria, testing frequency, result provision etc. This must be aligned to the company's Disaster Recovery policy and standards.
- b) IT MUST ensure that third parties undertake Disaster Recovery testing at least annually and be provided with a detailed report on the findings. IT MUST also be confident that third party Disaster Recovery Plans are current.
- c) IT SHOULD ensure that third party Disaster Recovery provisioning aligns to their respective Disaster Recovery policy and plan(s). Where there are differences, these MUST be managed as risks according to IT Risk Management Policy.

18 Logging and Monitoring

The purpose of this section is to provide a formalized approach to address the requirements for logging and monitoring of information systems.

Log management ensure that computer security records are stored in sufficient detail for an appropriate period of time. Log management activities include log generation, transmission, storage, analysis, and disposal; while protecting the confidentiality, integrity, and availability of logs.

18.1 Time Synchronization

- a) Time signals received from external sources **MUST** be synchronize with local time zone.
- b) Other internal servers **MUST** receive time signal only from central time servers located in KSL's infrastructure.
- c) The time-synchronization settings **MUST** be protected from unauthorized access and change. This includes parameters and methods used to set the system's clock.
- d) Any change in time settings **MUST** be logged, monitored and reviewed.

18.2 Audit Logging

- a) Audit trails generated **MUST** include but are not limited to the following events:
 - Individual accesses
 - Actions taken by any user with root or administrative privileges
 - Access to audit trails
 - Invalid access attempts
- b) Each record **MUST** include but is not limited to the following entries to have sufficient details in case of security breach:
 - User identification
 - Type of event
 - Date and time
 - Success or failure indication
 - Origin of the event
 - Identification or name of the affected resource (data, system component, etc.)
- c) Specifics measures **MUST** be taken for fault logging:
 - Error logging **MUST** be enabled if the function is available.
 - The level of error logging required **MUST** be determined by the custodians.
 - Faults **MUST** be logged and analyzed to take appropriate actions and resolution.

18.3 Log Review

- a) Logs must be reviewed by the custodians whenever there is a need for an investigation.
- b) The personnel involve in the log review activity **MUST** understand the threats faced by systems.

- e) The personnel detecting suspicious activities through the log review activity MUST follow the company's IT Incident Management process or go through via the Group IT's service desk to escalate.

18.4 Log Monitoring

- a) The level of monitoring required for each system components MUST be determined by the system custodians.
- b) The log monitoring activity should include, but is not limited to the following domains:
 - Authorized access
 - Operations performed
 - Unauthorized access attempts
 - System alerts or failures

18.5 Audit Log Protection

- a) The viewing of audit log files MUST be limited authorized personnel with a job-relation need.
- b) Audit log files MUST be protected from unauthorized modifications. This protection may include but is not limited to access control mechanisms, physical segregation, and network segregation.
- c) External-facing equipment MUST write logs onto a log sever located on a secured network.
- d) File-integrity monitoring or change-detection software MUST be used to ensure that audit trail files cannot be modified without generating an alert. However, addition of new log MUST not cause an alert.

19 Security Awareness Training

This section highlights the importance of security awareness and ongoing training for employees. It also outlines the company's approach to educating employees about security risks, policies, and best practices to promote a security-conscious culture.

19.1 Cyber Awareness Training

- a) Group IT will initiate mandatory cyber awareness training every **two (2)** months or **six (6)** times annually for the company.
- b) All training attendance **MUST** be monitored, tracked, and reported to the Management for its status and follow-up.
- c) All staff with access to Information system **MUST** attend the mandatory cyber awareness training as arranged.
- d) Selection of training modules or topic must be discussed and agreed upon by Group IT Management.

19.2 Cyber Phishing Simulation

- a) Group IT will initiate cyber phishing simulation bi-annually or **twice (2)** annually.
- b) All phishing simulation results must be monitored and reported to the Management for its status.
- c) Selection of phishing simulation topic must be discussed and agreed upon by Group IT Management.
- d) Users who failed the phishing simulation will be required to complete re-training exercise to strengthen their training and knowledge.

20. 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.

21. Reporting for Violations

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

22. 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.