INFORMATION SYSTEM SECURITY POLICY

Introduction
The purpose of Information System Security Management (ISSM) is to ensure BAU (Business as Usual), BC (Business Continuity) and to eliminate any negative impact on daily business operations by preventing and/or minimizing incidents related to Security breach or attacks. Information System Security Management enables a mechanism for information sharing which ensures the protection of information and systems related to information. The three basic components of Information System security management are:

1) ***Confidentiality*** – protecting sensitive information from unauthorized access and/or disclosure.
2) ***Integrity*** – safeguarding the accuracy and completeness of information and computer software.
3) ***Availability*** – ensuring that information and vital services are available to business users as and when needed.

Scope
The information security policy, its related standards and procedures applicable to all the permanent staff, contract staff, interns, other contract or temporary staff (collectively called "Staff") working in RCL Group with access to RCL device and/or Information Systems. It is applicable to all the computer equipment, whether connected to RCL network, and the information and software stored on that equipment.

Definition
"**RCL**" means management of RCL Group and / or its related companies.

"**Management**" means management of the Company.

"**Staff**" means all permanent staff, contract staff, interns, other contract or temporary staff.

"**Information**" implies sensitive information that is proprietary; trade secrets of the RCL's business and / or that will threaten the RCL business advantage if made known to others by knowingly/unknowingly in the same industry or industry in general.

"**Security incident**" means any event that has/ or could have resulted in loss or damage to RCL assets, or an incident that is in breach of RCL information security procedures or rules and regulations governing the use of information systems and services.

"**Administrator**" means the staff appointed by the Management to manage a particular information resource.

Staff Practices
Every member of staff and others with access to RCL equipment should have access to a copy of the Information Security policy. Others that have access to RCL system will sign an agreement that they accept the RCL policy on information security, confidentiality, regulations and the responsibilities concerning information systems and services.

All the Staff members will be issued with the policy and the regulations governing the use of information systems and associated equipment.

All the new Staff members will be briefed on the importance of information systems security and their role during orientation.

The Network and Information System Administrator will be notified of every staff transfer, promotion and termination to adjust information systems access privileges as appropriate.

The VP (Group IT) of RCL is responsible for information system security practices relating to Staff.

Staff Responsibility
Information system security is the responsibility of each Staff of the organization.

Information carried outside office premises in any form must not be left unattended and/or make it vulnerable to theft whether physically or by duplication(copying). These include hard copies, soft copies in the form of files or information stored in Company computer notebooks on loan to staff.

No Staff shall divulge confidential information to outsiders or other staff who are not authorized to obtain that information.

RCL information systems resources shall only be used for purposes related to RCL business.

Stealing or copying software is illegal and can serve as grounds for prosecution and it may also lead to termination of services.

Staff are also responsible for reporting any security incidents of which they become aware through the appropriate channels. Some of the examples are computer fraud, phishing, viruses and network penetration.

All Staff must report suspected security breaches to their immediate supervisor and/or to the designated Security Administrator. Once notified, immediate supervisor must notify the appropriate security administrator of the reported security incident.

Managers/Immediate Supervisor are responsible for keeping higher management informed of security incidents. The security administrator will investigate, research, resolve and document the incident. When necessary, the Security Administrator would provide advice/measures to contain incidents, and staff should implement such without fail.

Human Resource Security

Prior to employment

To ensure that staff and contractors understand their responsibilities and are suitable for the roles for which they are considered.

1 Screening

Control

Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks

Implementation guidance

Verification should consider all relevant privacy, protection of personally identifiable information and employment-based legislation, and should, where permitted, including the following:

a) Availability of satisfactory character references, e.g. one business and one personal.

b) A verification (for completeness and accuracy) of the applicant's curriculum vitae.

c) Confirmation of claimed academic and professional qualifications.

d) Independent identity verification (passport or similar document).

e) More detailed verification, such as credit review or review of criminal records.

When an individual is hired for a specific information security role, organizations should make sure the candidate:

a) Has the necessary competence to perform the security role.

b) Can be trusted to take on the role, especially if the role is critical for the organization.

Where a job, either on initial appointment or on promotion, involves the person having access to information processing facilities, and in particular, if these are handling confidential information, e.g. financial information or highly confidential information, the organization should also consider further, more detailed verifications.

Procedures should define criteria and limitations for verification reviews, e.g. who is eligible to screen people and how, when and why verification reviews are carried out.

A screening process should also be ensured for contractors. In these cases, the agreement between the organization and the contractor should specify responsibilities for conducting the screening and the notification procedures that need to be followed if screening has not been completed or if the results give cause for doubt or concern.

Information on all candidates being considered for positions within the organization should be collected and handled in accordance with any appropriate legislation existing in the relevant jurisdiction. Depending on applicable legislation, the candidates should be informed beforehand about the screening activities.

2 Terms and conditions of employment

Control

The contractual agreements with staff and contractors should state their and the organization's responsibilities for information security.

Implementation guidance

The contractual obligations for staff or contractors should reflect the organization's policies for information security in addition to clarifying and stating:

a) That all staff and contractors who are given access to confidential information should sign a confidentiality or non-disclosure agreement prior to being given access to information processing facilities.

b) The staff or contractor's legal responsibilities and rights, e.g. regarding copyright laws or data protection legislation.

c) Responsibilities for the classification of information and management of organizational assets associated with information, information processing facilities and information services handles by the staff or contractor.

d) Responsibilities of the staff or contractor for the handling of information received from other companies or external parties.

e) Actions to be taken if the staff or contractor disregards the organization's security requirements (see Disciplinary process)

Information security roles and responsibilities should be communicated to job candidates during the pre-employment process.

The organization should ensure that staff and contractors agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the organization's assets associated with information systems and services.

Where appropriate, responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of the employment (see Termination and change of employment).

Other information
A code of conduct may be used to state the staff or contractor's information security responsibilities regarding confidentiality, data protection, ethics, appropriate use of the organization's equipment and facilities, as well as reputable practices expected by the organization. An external party, with which a contractor is associated, can be required to enter contractual arrangements on behalf of the contracted individual.

During employment

To ensure that staff and contractors are aware of and fulfil their information security responsibilities

1 Management responsibilities

Control
Management should require all staff and contractors to apply information security in accordance with the established policies and procedures of the organization.

Implementation guidance
Management responsibilities should include ensuring that staff and contractors:

a) Are properly briefed on their information security roles and responsibilities prior to being granted access to confidential information or information systems.

b) Are provided with guidelines to state information security expectations of their role within the organization.

c) Are motivated to fulfil the information security policies of the organization.

d) Achieve a level of awareness on information security relevant to their roles and responsibilities within the organization (see Information security awareness, education and training).

e) Conform to the terms and conditions of employment, which includes the organization's information security policy and appropriate methods of working.

f) Continue to have the appropriate skills and qualifications and are educated on a regular basis.

g) Are provided with an anonymous reporting channel to report violations of information security policies or procedures ("whistle blowing").

Management should demonstrate support for information security policies, procedures and controls, and act as a role model.

Other information

If staff and contractors are not made aware of their information security responsibilities, they can cause considerable damage to an organization. Motivated personnel are likely to be more reliable and cause fewer information security incidents.

Poor management can cause personnel to feel undervalued resulting in a negative information security impact on the organization. For example, poor management can lead to information security being neglected or potential misuse of the organization's assets.

2 Information security awareness, education and training

Control

All staff of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organization policies and procedures, as relevant for their job function.

Implementation guidance

An information security awareness programmed should aim to make staff and, where relevant, contractors aware of their responsibilities for information security and how those responsibilities are discharged.

An information security awareness programmed should be established in line with the organization's information security policies and relevant procedures, taking into consideration the organization's information to be protected and the controls that have been implemented to protect the information. The awareness programmed should include a number of awareness-raising activities such as campaigns (e.g. an "information security day") and issuing booklets or newsletters.

The awareness programmed should be planned to take into consideration the staff roles in the organization, and, where relevant, the organization's expectation of the awareness of contractors. The activities in the awareness programmed should be scheduled over time, preferably regularly, so that the activities are repeated and cover new employees and contractors. The awareness programmed should also be updated regularly so it stays in line with organizational policies and procedures and should be built on lessons learnt from information security incidents.

Awareness training should be performed as required by the organization's information security awareness programmed. Awareness training can use different delivery media including classroom-based, distance learning, web-based, self-paced and others.

Information security education and training should also cover general aspects such as:

a) Stating management's commitment to information security throughout the organization.

b) The need to become familiar with and comply with applicable information security rules and obligations, as defined in policies, standards, laws, regulations, contracts, and agreements.

c) Personal accountability for one's own actions and inaction, and general responsibilities towards securing or protecting information belonging to the organization and external parties.

d) Basic information security procedures (such as information security incident reporting) and baseline controls (such as password security, malware controls and clear desks).

e) Contract points and resources for additional information and advice on information security matters, including further information security education and training materials.

Information security education and training should take place prosaically. Initial education and training apply to those who transfer to new positions or roles with substantially different information security requirements, not just to new starters and should take place before the role becomes active.

The organization should develop the education and training programmed to conduct the education and training effectively. The programmed should be in line with the organization's information security policies and relevant procedures, taking into consideration the organization's information to be protected and the controls that have been implemented to protect the information, the programmed should consider different forms of education and training, e.g. lectures or self-studies.

Other information

When composing an awareness programmed, it is important not only to focus on the 'what' and 'how', but also the 'why'. It is important that staff understand the aim of information security and the potential impact, positive and negative, on the organization of their own behavior.

Awareness, education d training ca be part of, or conducted in collaboration with, other training activities, for example general IT or general security training. Awareness, education, and training activities should be suitable and relevant to the individual's roles, responsibilities, and skills.

An assessment of the staffs' understanding could be conducted at the end of an awareness, education, and training course to test knowledge transfer.

3 Disciplinary process

Control

There should be a formal and communicated disciplinary process in place to take action against staff who have committed an information security breach.

Implementation guidance

The disciplinary process should not be commenced without prior verification that an information security breach has occurred.

The formal disciplinary process should ensure correct and fair treatment for staff who are suspected of committing breaches of information security. The formal disciplinary process should provide for a graduated response that takes into consideration factors such as the nature and gravity off the breach and its impact on business, whether this is a first or repeat offence, whether the violator was properly trained relevant legislation, business contracts and other factors as required.

The disciplinary process should also be used as a deterrent to prevent staff from violating the organization's information security policies and procedures and other information security breaches. Deliberate breaches may require immediate action.

Other information
The disciplinary process can also become a motivation or an incentive if positive sanctions are defined for remarkable behavior with regards to information security.

Termination and change of employment
To protect the organization's interests as part of the process of changing or terminating employment.

1 Termination or change of employment responsibilities

Control
Information security responsibility and duties that remain valid after termination or change of employment should be defined, communicated to the staff or contractor, and enforced.

Implementation guidance
The communication of termination responsibilities should include on-going information security requirements and legal responsibilities and, where appropriate, responsibilities contained within any confidentiality agreement and the terms and conditions of employment (see Terms and conditions of employment) continuing for a defined period after the end of the staff or contractor's employment.

Responsibilities and duties still valid after termination of employment should be contained in the staff or contractor terms and conditions of employment (see Terms and conditions of employment).

Changes of responsibilities or employment should be managed as the termination of the current responsibility or employment combined with the initiation of the new responsibility or employment.

Other information

The human resource's function is generally responsible for the overall termination process and works together with the supervising manager of the person to manage the information security aspects of the relevant procedures. In the case of a contractor provided through an external party, this termination process is undertaken by the external party in accordance with the contract between the organization and the external party.

It may be necessary to inform staff, customers or contractors of change to personnel and operating arrangements.

Access to Equipment

Only authorized Staff whose job scope requires, will be allowed access to information systems resources. All information systems resources will be protected against fire, water, electric power fluctuations, physical damage, and/or theft.

All the servers and other sensitive pieces of hardware should be kept in locked rooms.

All the computers room must be placed in rooms with card key access and/ or physical key.

All the visitors to the computer room must sign in at the security access point.

Access to Data

All the data files on RCL information systems will be protected against unauthorized changes. Sensitive data files will be protected against unauthorized reading and copying.

RCL information systems shall be programmed to control, which User Ids can read, and which ones can write to any given files. Every file shall be associated with an owner. Unless otherwise specified. The owner of each file is responsible for specifying whether the file is sensitive and which User IDs should be allowed to read or write to it.

Security administration activity should be recorded.

Access to On-line System

Access to an on-line system is allowed only to Staff's User IDs, which have been authorized to those systems.

Techniques will be used to control access to on-line systems - Physical barriers, access control software, 2 Factor Authentication system, restriction of sensitive transactions to specified systems.

Staff should not send any data over the Internet in clear text. Data must be encrypted by an approved, strong encryption software.

Access Network Resources

Measures must be taken to protect network resources from authorized access. Access to Database shall be restricted, it will be allowed only to authorized staff upon approval from designated approval party.

The system's security features shall have the technical ability to restrict access to such information that is necessary for the staff's operations. The system shall be configured to protect resources from unauthorized access.

Systems users shall be restricted to only those privileges necessary to perform assigned tasks as per their job scope. Only authorized users shall have access.

Access to configuration and/or network management shall be restricted.

User Identification and password

No outsider should be allowed to access RCL information systems resources without authorized user identification (User ID) and password. User IDs are made available to staff as part of the process of providing users with necessary network services.

User identification shall be authenticated before the system may grant user access to systems/network. Each member of staff is responsible for all the activities which occur under the auspices of their user id.

User ID's will be removed when staff resigned/employment is terminated and/or transferred to a position where access to the system is no longer required. The User ID's will be removed/disabled if they are not accessing the system for ninety (90) days or more. Will be disabled when an incorrect password is entered 5 consecutive times.

Passwords must be individually owned and maintain its confidentiality. Staff must change his or her password at least once every 90 days. Password should contain minimum of six characters and contain alphanumeric characters.

Passwords must not be shared with others, same as user id or names of person, place or things that closely identified with the user.

No	Password Parameter	Description	Setting
1	Account lockout duration	Specifies the number of minutes before a locked user can be unlocked automatically by the system.	5 minutes
2	Account lockout threshold	Specifies the number of failed login attempts allowed before the account is locked out.	5 unsuccessful logon attempts
3	Idle session timeout	Specifies the period which a session with no activity should remain connected.	30 minutes
4	Minimum Password Age	Stipulates how many days a user must keep new passwords before they can change them.	1 day
5	Maximum Password Age	Stipulates how many days a user can use the password before the system requires to change it	90 days
6	Password history	Specifies the number of unique new passwords a user must use before an old password can be reused.	5 passwords remembered

Note:

a) Password policy is exempted for Microsoft SQL Server version 2008 and earlier which has the limitation to implement the policy.
b) Password policy is exempted for systems with Windows Operating System version 2008 and earlier which has the limitation to implement the policy.
c) Password policy is exempted for non-windows. Means those Systems with operating system other than Windows, it should be excluded from the said password policy. The default password policy on the Non-Windows shall prevail.

Critical system passwords are managed by the Head of IT Infrastructure and a copy is retained in a safe/ offsite Password Vault with VP (Group IT).

Upon request from department head/immediate supervisor and/or HR Department via IT Service Desk, ID and password will be terminated for resigned staff or transferred staff to stop the required server resources and the related Information access.

Protection of Information and systems from threats:

All Information assets vulnerable to virus infection or attack must be installed with protection software or device specified where applicable.

Latest patch updates of such protection feature must be performed to reduce vulnerabilities to fresh virus attacks daily or as and when advised through channels established by the Management.

Review and update anti-virus program will take place on a regular basis.

Operating System patches on servers to be installed manually only after thorough review and ensure that the patches are currently supported by the product owners to avoid any risk arising due to auto-updating of patches.

Use of Internet

Grant of Internet usage in the Company is limited to a 'required for work' basis and subjected to the recommendation of department head/Immediate Supervisor and/or approval by the Management.

Staff who can access the Internet must adhere to the policy of work-related access, whether while surfing for research, checking, transacts on other Internet sites or exchanging mails with external parties or mail messaging systems. This applies to all incoming or outgoing communications with Internet access.

Staff who can access Internet must not engage in undesirable communications like access to pornographic sites or distributing any non-work-related mails. The latter shall include but is not limited to pornographic material, chain mails, screen savers and graphic pictures.

Remote Access

Grant of remote access using VPN is subjected to requirement to connect to central server(s) for processing as approved by Management. This requires the installation of a proprietary VPN client arranged by the IT infrastructure support team.

Backup of Information

Backup of Information shall be performed daily and should be kept for a period of minimum seven (7) days or otherwise specified by Administrators.

Unauthorized Software

Installation of any software must be performed by RCL IT support team. Software other than those installed by the IT team are deemed 'unauthorized'. An annual inventory

audit is conducted by the IT team to ensure compliance. Perpetrators will be reported to Management for disciplinary action.

Security Breach:
Security breach occurs when staff knowingly distributes Information to parties who are not rightful recipient(s) of such Information.

Due diligence is not exercised on the part of staff to ensure that the Information in their possession is protected to the best of their ability.

Upon advice by the established channels of the Company, staff persist in not rectifying security breach or potential security breach situation.

Contingency Planning
Information owners are responsible for developing and co-ordination disaster recovery plan in the event of a short-term loss or the destruction of the RCLs information systems processing for which they are responsible.

Review and testing of the disaster recovery plan should take place on an annual basis.

Disciplinary Action
Where there is an Information security breach due to negligence or by malicious intent of staff, Company has the right to ban the usage of such Information by the staff and exercise disciplinary actions up to and including termination of service.

Any staff found guilty of being perpetrators of the Information breach may at the discretion of the Company be liable for immediate dismissal without notice. This will supersede any other conditions specified for termination of service with the Company.

Where the security breach includes criminal related activities like pornography, staff will be liable for immediate dismissal without notice and related criminal evidence shall be handed over to official authorities for further action.

Document Review Policy
This document is to be reviewed on an annual basis.
The Executive committee of Information Security has authority to revise the policy.

Revision	Release Date	Summary of Change
1.0	1st May 2019	NA
2.0	1st Nov 2021	Human Resource Security
2.1	30th Sep 2022	NA
3.0	30th Sep 2023	Password expiry
4.0	10th Oct 2024	Password Policy Exception Windows Patches Exception
4.1	4th Apr 2025	Document review policy

PREPARED BY:	SIGNATURE
Name: Patrick Png **Title:** Assistant General Manager (Head of IT Infrastructure)	7 April 2025
APPROVED BY:	**SIGNATURE**
Name Chatgamol Phitaksutee **Title:** Vice President (Group IT)	
ENDORSED BY:	**SIGNATURE**
Name: Dr.Twinchok Tanthuwanit **Title:** President (RCL Group)	