INFORMATION SYSTEM SECURITY POLICY

Policy Objectives

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 enable 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.

The overall framework for particular security policies, system-specific security requirements, and departmental/local processes is defined in this policy. All derived security standards, guidelines, rules, and practices must adhere to the current policy statement.

Scope of the Policy

This policy is an essential component of the RCL Group Business Code of Conduct and 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.

This policy addresses the security of RCL Group-owned or operated data networks and information systems, as well as the transfer, or process of data stored in those systems.

Security concerns pertaining to general building and physical safety are not covered by this policy. It does, however, address the physical security features of structures or specific building components that have an immediate impact on the protection of RCL Group-owned data.

Policy

This policy aims to minimize cyber security risks while assisting in making the most efficient use of the computer resources available. Staff ought to be aware of the following:

- It is your personal responsibility to safeguard the hardware, software, and data that you handle. Everyone bears responsibility for security.
- Identify which information is not available to the public. This includes customer, personal, and company-secret information, all of which are further explained below. Ask if you are unsure or do not know. Information, even though it is immaterial, can nevertheless be an asset.
- Only use the resources at your disposal to advance RCL Group's interests.
- Recognize that your actions on the system are your responsibility.
- Prevent loss and theft of equipment. Store information only on secured devices.
- Do not bypass established network and internet access connection rules.
- Do not disable or remove firewall or virus detection software.
- Do not install or alter any unapproved software or "plug-ins" for your browser.
- Do not copy or store RCL Group data on unapproved external places or devices, including cloud-based services that have not been permitted by the organization. When this is required, get in touch with IT to find the best way to transfer files securely.
- It is imperative that you report any prospective or real security issue as soon as you become aware of it by sending an email to itnet@rclgroup.com or call IT Infrastructure Department.

Staff are required to read, comprehend, accept, and abide by the Policies and corresponding Standards included in this session. These establish the guidelines that RCL Group follows when operating and protecting its data and information systems in order to reduce risk and minimize the impact of any potential incidents.

Data Protection

The RCL Group Information Management Policy is supported by data protection standards that must be followed in order for the security measures outlined in this policy to be implemented. RCL Group takes the protection of personal data seriously.

Human Resource Security

1. Job definition and resourcing

The Group's Security Human Resources policy and standards must address information security. At the very least, the HR policies should guarantee that job descriptions sufficiently address security, that staff undergo appropriate screening and training, and that all new hires and contractors sign confidentiality agreements.

2. **User training on Security Awareness**
   To guarantee that the appropriate degree of Cyber Security Awareness is established and upheld within the company, a training program and accompanying materials need to be in place. 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.

IT Asset Management

RCL Group makes use of a wide range of information assets, including servers, laptops, and desktops. An inventory of all important information assets owned or utilized by the organization must be kept up to date and contain the following information:

- Asset type and attributes.
- Data owner.
- The custodian of the data and the location of the repository (database, etc.).
- The sensitivity of the asset, due to regulations, laws, customer expectations or other requirements.
- Requirements for the asset regarding availability, uptime, business continuity, etc.

Hardware Management

RCL Group handle hardware using a hardware lifecycle approach:

- Only authorized and appointed vendors used to purchase hardware;
- New hardware should only have authorized software configurations applied to it, and end users should handle any hardware that is provided to them with care.
- Hardware that is lost or stolen needs to be notified right away;
- End-of-life hardware should be disposed securely.

Information Management Policy

1. **Information Classification**
   The RCL Group information security policy prioritizes data privacy protection while safeguarding the three elements of information held on RCL Group systems: **Confidentiality**, **Integrity**, and **Availability.** To enable the execution of the proper levels of security in accordance with its criticality and to guarantee that the controls applied to it are adequate and do not hinder the company's activity, all RCL Group information must be categorized based on these three categories. The RCL Group

Information Management Policy contains specific rules for information classification.

2. **Information Handling**

Information should be managed in both physical and electronic versions according to its classification, sensitivity, and risk:

- Verify the existence of confidentiality agreements before disclosing any external data.
- Before transmitting any files, verify email addresses.
- Only transfer files to removable storage when absolutely required and encrypt the storage.
- Use restricted access storage areas such as O365 SharePoint whenever possible.
- Data disposal should be done in accordance with the Information Asset Handling and Protection Standard for End User

<u>System Access Policy</u>

Access to data and systems owned or controlled by RCL Group must be granted on the basis of least privilege and need to know.

Access control systems is allowed only to Staff's UserIDs, which have been authorized to specified systems.

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

Multi factor authentication for remote access to corporate and production networks by staff, administrators, and third parties will be required.

When controlling user access permissions, the following guidelines must be followed:

- User registration: authorizing and distributing access privileges to users on need-to-know basis.
- Handling privileges. Every system needs to have distinct hierarchies, and each hierarchy needs to have official approval.
- Administration of users. As mentioned, every system needs explicit approval processes and ways to provide access to it. Every system needs to have joiner, mover, and leaver procedures with audit trails.
- User access rights are subject to periodic reviews.

- User accounts that are not inactive need to be disable/ remove automatically after 90 days.

User Authentication Standard

It is imperative that users be forced to update their passwords on their initial login and every 90 days thereafter.

Passwords shall not be displayed or transmitted in clear text and shall be suitably protected via approved encrypted solutions.

Passwords is required to be kept in an encrypted manner. A history of 5 passwords must be kept in order to prevent password reuse.

Maximum of 5 unsuccessful attempts to log in, the account will be locked until an administrator unlocks it.

Default accounts shall be disabled and/or default passwords associated with such accounts shall be changed.

Password Selection

To increase the difficulty of guessing or stealing your passwords, please remember the following:

- Avoid using dictionary words—all real words are simple to figure out. Do not use any expletives, foreign phrases, slang, names, nicknames, or other language-specific terms.
- Use a combination of uppercase, lowercase, digits, and special characters. Alternatively, try using acronyms that are specific to you alone, mnemonics, random letters, etc., and insert nonalphabetic characters in the center of the word.
- Pick something you will remember. If your strong password is scribbled on a Post-It note and sitting on your desk, it is useless! Choose a hint or reminder that is so mysterious that only you can decipher.
- Do not share your password with anyone or let them log in as you.
- Make an effort not to let anyone to witness you enter your password. Select an item that is difficult to infer from them observing.
- If available, make use of multi-factor authentication. This is a combination of something you know (password, for example), your possessions (token, smartphone, etc.), and/or your identity (biometric, fingerprint, for example).

Acceptable Use Policy

The RCL Group may only use corporate IT resources for business-related activities. You can find the detailed requirements in the dedicated policy named RCL Group Acceptable Use Policy.

1. **Email Usage**
   E-mail is a business communication tool which all RCL Group staff are requested to use in a responsible, effective, and lawful manner.

2. **Internet Usage**
   All staff at RCL Group have access to the Internet to help them with their daily tasks, which include researching suppliers, goods, government data, and other work-related information.

   Periodic and restricted personal usage of the Internet is allowed if such use does not:
   - Affect productivity and work performance.
   - Consist of downloading or sharing huge files.
   - Have an adverse effect on the IT system performance of RCL Group.
   - The following rules should be followed when using Internet access facilities.
   - Limit how much time you spend on the Internet for yourself.
   - Verify that any data you obtain from the internet is true, comprehensive, and up to date.
   - Respect the licensing, copyright, data, and software protections granted by law.
   - Report any unusual events to the security team immediately.
   - Avoid downloading or sharing texts or photos that include software, offensive, threatening, racist, or politically extreme content, or that encourage violence, hatred, or unlawful action.
   - Avoid using business property to gain illegal access to any other computer system or network.
   - Avoid portraying yourself as someone else.
   - Uploading confidential company information to external file storage services, such as Dropbox, or Google Drive, is strictly prohibited.
   - User documentation, source code, object code, and all other information related to software development.
   - Project related information.
   - Business plans and company strategy.
   - Configurations of the corporate IT infrastructure, including log files.
   - Intellectual property includes trade secrets, patents, and copyrights.

- Personal data on staff, including pay, appraisals, health records, and medical information.
- Any information pertaining to clients and potential clients, such as project specifications, proposals from clients, agreements, costs, or strategic strategies.
- Customer-related data, including any information kept in RCL Group software, like bank account or transaction information.
- Any other company non-public information.

3. **Portable Media**
   It is not allowed to utilize portable media such as USB storage. The goal is to prevent unauthorized parties from transferring company and customer information. Any portable media used on RCL Group network may be inspected and deleted at RCL Group's sole discretion.

Remote Access and Electronic Communication

Users, such as traveling staff and/or consultants, will frequently need to access the RCL Group's information systems from locations other than the office.

Only the facilities officially approved and supported by the internal IT department may be utilized for remote access to the Corporate IT Infrastructure resources (i.e., RCL Group Secure Access Portal and/or Virtual Private Network). The associated security policies must be applied.

Use of RCL Group-approved communication channels is restricted to online interactions between RCL Group offices and external parties. It is completely forbidden to use personal remote access connections, personal VPNs, or any other type of connectivity equipment that insecure the RCL network.

The RCL Group Network and Communications Policy is the specific policy that outlines the requirements for electronic communication in detail.

System Changes and Configuration

Although unmanaged change can pose serious security concerns to RCL Group, the company acknowledges that change is an essential process for maintaining, safeguarding, and improving services offered to clients. The RCL Group is aware that there are various kinds of change, and that in order to address each form of change in the best possible way, an effective change management strategy needs to be put in place.

All changes must follow the IT System Configuration Standard and IT Change Management Standard, and they must be carried out in a regulated and authorized manner.

Changes to the system or reconfiguration of common IT components are prohibited. IT and/or System admin can modify or install software components on workstations in accordance with the specifications of projects. Changes to the following systems are absolutely forbidden.

- Installation of:
  - Unauthorized connectivity devices, such as data modems and/or switches;
  - any component that able to gain authorize access to restricted areas;
  - any non-standard hardware or software component.

- Disable antivirus software.

<u>Network and Communication Policy</u>

1. **Internet Usage**

   RCL Group has 26 regional offices that are a component of our regional network, a secure network is essential to the security of our business:

   - Networks that face the external should have a firewall installed.
   - Only authorized personnel can make changes to the network's logic and configuration.
   - Networks ought to be divided based on geography and/or business link.
   - Appropriate controls ought to be in placed at network interfaces.
   - WAN services should only be acquired through selected approved vendors.
   - Implementing network event logging and monitoring is recommended.
   - Third-party users are not authorized to connect their computing devices to the RCL Group's wired or wireless network, unless authorized.
   - Networks and computers owned by the RCL Group may only be connected to those of third parties with permission once it has been established that the systems adhere to RCL Group security regulations.

2. **Wireless Networks**

   - Guest wireless network passwords should be reset frequently.
   - Use only authorized wireless access points.
   - Wireless networks should be always encrypted.

Threat and Incident Management Policy

1. Event Logging and Monitoring

It is necessary to put in place sufficient monitoring measures to identify intrusions and illegal access to its information processing systems. Risk assessment will identify the necessary level of monitoring, and any pertinent or applicable legal requirements will be identified to make sure the monitoring operations adhere to the requirements.

Activities that fall under the category of monitoring include reviewing:

- An automated intrusion detection system log.
- Firewall logs.
- User access logs.
- Network logs.
- Applications logs.
- Help desk Tickets.
- Cybersecurity Assessment.
- Additional error and log files.

The IT Infrastructure Department will be notified of any security vulnerabilities found and will conduct an investigation.

2. User Monitoring

RCL Group monitors a variety of user behavior factors, including but not limited to the following, to preserve the security of the Group's IT systems (including thwarting cybersecurity threats) and to safeguard the Group's assets and data.

- Monitoring the use of the Internet.
- Reviewing content that has been posted or downloaded from the Internet.
- Reviewing emails that users send or receive in the event that there is a reasonable suspicion that any of the terms of this policy, the laws that apply, or any legal or regulatory requirements have been violated.
- Reviewing the installed software on the computers of users.
- PC usage and network logins for RCL Group.

Workstation Security

Workstations include laptops and desktops:

- Antivirus software that has been approved by the company should be installed and enabled on every workstation.
- Data loss prevention software should be deployed on all workstations. Encryption should be used on all laptops.
- Install software only from trusted sources.

- Do not allow unauthorized user from using your workstation.
- Take necessary actions to keep your workstation physically safe.

Bring Your Own Device

The only devices that are accepted for direct connections to the RCL Group Local Area Network (LAN) are those that are owned by the RCL Group. By default, all non-RCL Group owned devices are regarded as untrusted. Never connect an untrusted device directly to the RCL Group internal network, either via the staff wireless network or a network cable connection in an RCL Group office. When in an RCL Group office, untrusted (non-owned by the group) devices are restricted to only using the visitor network and/or wireless network for Internet access only. It is not permitted for staff to link their personal devices to the corporate network of RCL Group.

Licensing

RCL Group utilizes software from various third-party sources, which is copyrighted by the respective developers. Unless explicitly authorized, staff are prohibited from reproducing copies of the software. The policy of RCL Group is to uphold and comply with all copyrights pertaining to computer software, as well as adhere to the terms outlined in software licenses.

Furthermore, RCL Group is committed to effectively managing its software assets and ensuring the installation and usage of exclusively legitimate software on its workstations and servers.

Backup

Backup within the RCL Group Business Continuity Management Policy establishes a framework to safeguard information covered by this policy from loss during incidents impacting availability or integrity. It is imperative that all storage media containing backups of RCL Group data adhere to the data classification standards related to Data Confidentiality, Integrity & Availability, while prioritizing data privacy.

Asset owners are tasked with determining both the data classification and backup necessities, which must then be communicated to IT for implementation. Written notification outlining specific backup requirements for each asset or data set, including the designated backup retention period aligned with the Group Business Continuity Management Policy (BCMP), is the responsibility of asset/data owners to provide to Corporate IT.

Third Party Risk Management Policy (incl. Cloud Computing)

The Third Party Risk Management policy delineates the prerequisites for conducting IT operations with external parties, encompassing Cloud Computing services. The necessary processes and controls aimed at mitigating risks associated with IT outsourcing initiatives, including Cloud Computing arrangements, are thoroughly outlined in the RCL Group IT Outsourcing Policy. This policy applies uniformly to all RCL Group staff and contractors engaged with external IT service providers.

Malware Protection

It is imperative to uphold a stringent process to prevent the infiltration of malicious software into the group's secure IT infrastructure. This entails regular updates of anti-malware software, scheduled malware scans, and vigilant monitoring of events and incidents associated with malware, as specified in the RCL Group Threat and Incident Management Policy.

Security Incident Management

RCL Group adheres to a consistent and efficient protocol for addressing any confirmed or potential security incidents concerning its information systems and data. The Security Incident Management Standard outlines the framework for early detection, reporting, and response to such incidents. It is imperative that all security incidents, whether confirmed or suspected, be promptly reported by sending an email to itnet@rclgroup.com.

Even if a security incident is perceived as minor, it should be reported without delay, as it could potentially be indicative of a broader issue or trend. Furthermore, initial assessments of the severity of a security incident may be misleading and may not accurately reflect the underlying risk's seriousness.

Business Continuity Management

RCL Group upholds a comprehensive Business Continuity Management Policy (BCMP), which mandates sub-functions to formulate thorough business continuity plans within its framework. Specifically, the IT function is tasked with ensuring that the Business Continuity Plan sufficiently encompasses the continuity of the group's IT infrastructure.

Disaster recovery planning (DRP) is an integral component of the broader BCP framework. Recognizing its significance, the essential characteristics of a disaster recovery plan are elaborated upon below. There are various categories of disruptive events covered by our BCP/DRP:

- Loss of data, which may include loss of program and system files;
- Unavailability of computer and network equipment.
- Environmental disasters
- Organized/deliberate disruption
- Loss of utilities/services
- Equipment/system failure
- Pandemics
- Cyber Attacks
- Other (health and safety, legal, etc.)

The determination of recovery requirements falls upon the asset owner, contingent upon the criticality of the processes within the Business Functions utilizing the IT systems, as identified through Business Impact Analysis.

- Adequate recording of every disaster recovery plan, which is necessary to facilitate the plans' effective implementation.
- A disaster recovery plan that outlines the necessary security precautions to ensure the level of integrity and confidentiality needed for the systems that can be recovered.
- The Disaster Recovery Plan outlines a routine process for copying data so that originals can be recreated in the event of a calamity. Operational recovery will not be accomplished using disaster backups.
- Regular testing of the disaster recovery plan is necessary.

Physical Security Policy

Access to all RCL Group offices, server and/or equipment rooms, and other work areas housing sensitive information must be strictly limited to authorized personnel with a legitimate need for access. It is the responsibility of every RCL Group user to ensure that important information assets are not left unattended on desks, particularly outside of regular working hours. At RCL Group, our security relies on the physical protection of our resources, both at dedicated data centers and on-premises server and/or equipment rooms.

- Server and/ or equipment rooms ought to be situated in an area where the chance of natural disasters is within our tolerance for risk.
- Secure access control systems (face scan and/or finger scan and/or pin) should be installed at every point of entry to IT facilities.
- It is important to have appropriate environmental controls in place, such as air conditioning, fire suppression systems, water detection.
- Battery backup power must be available on-site for a long enough period of time to allow the conversion to diesel power generation if available.

- Access for visitors should be restricted
- Food and beverages are prohibited in the data centers of RCL Group.

Risk Management Policy

The foundation of our approach to identifying and addressing Information Security risks lies in our Information Security Risk Management framework. While centrally managed, our methodology relies on support from regional and divisional levels. Hence, it is essential for Management to acquaint themselves with the Risk Management Policy and understand their role within this framework.

Responsibilities

While Information Security is a collective responsibility, the ultimate accountability lies with the Board of Directors and Executive Management. This responsibility filters down through a hierarchy of designated roles within the organization.

1. **Chief Security Officer**

   The Chief Security Officer (CSO) bears several critical responsibilities within RCL Group:

   - Spearheading information security management across the organization, serving as a primary liaison on information security matters for both internal staff and external entities.
   - Executing and enforcing this policy alongside associated policies, standards, and guidelines.
   - Vigilantly monitoring and responding to potential or actual security breaches.
   - Ensuring that all staff members comprehend their roles and obligations concerning information security.
   - Offering specialized guidance and counsel on security matters.

2. **Security & Privacy Committee**

   The Security & Privacy Committee is tasked with overseeing information risk within RCL Group, advising executive management on the effectiveness of security and privacy management across the organization. Additionally, the committee ensures RCL Group's compliance with relevant legislation and regulations.

3. **Managers**

   Managers hold individual responsibility for the security of their respective environments where information is processed or stored. Additionally, they are tasked with:

   - Ensuring that all staff, whether permanent, temporary, or contracted, are fully informed about the information security policies, procedures, and user obligations relevant to their area of work, as well as their personal responsibilities for information security.

- Deciding the level of access to be provided to specific individuals.
- Providing appropriate training for staff members on the systems they utilize.
- Ensuring that staff members know how to seek advice on information security matters.

4. **All Staff**

   Every staff member holds responsibility for information security and must therefore comprehend and adhere to this policy and its associated guidance. Failure to comply may lead to disciplinary action. Specifically, all staff members should be aware of:

   - The nature of the information they handle, including how it should be utilized, stored, and transferred in terms of data security.
   - The procedures, standards, and protocols governing the sharing of information with external parties.
   - The process for reporting a suspected breach of information security within the organization.
   - Their duty to raise any concerns regarding information security.

All users within RCL Group are obligated to follow the provisions outlined in this Policy, along with all related policies, standards, guidelines, and procedures. They must promptly report any incidents of misuse or abuse of which they become aware, as described in the RCL Group Security Incident Management Policy.

5. **External contractors**

   Before external contractors are granted access to the organization's data or information systems, it is mandatory for contracts to be established and operational. These contracts must guarantee that the staff or subcontractors affiliated with the external organization adhere to all relevant security policies.

Breaches

This Policy will be treated with utmost seriousness and may lead to disciplinary measures in alignment with the legal and contractual obligations, potentially including termination of employment. Any user found to be in violation of the rules outlined in this Policy or relevant laws will be held fully accountable, and RCL Group will distance itself from the user to the fullest extent permitted by law.

All instances of policy breaches must be promptly reported to the respective Manager/Director for appropriate action. Additionally, all security incidents, whether confirmed or suspected, must be reported without delay by sending an email to itnet@rclgroup.com.

History

Prepared by	Revision	Release Date	Summary of Change
Patrick Png	1.0	1 May 2022	NA
Patrick Png	2.0	1 Nov 2023	Human Resource Security
Patrick Png	3.0	15 Mar 2024	Password expiry