Revisions

Date	Change	Version
12/18/2013	Version 1.0	1.0

The Information Security Policies are critical to the safeguarding of Royal Caribbean Cruises Ltd. (RCCL) corporate infrastructure, information, and customer data. This policy is intended to identify important areas that need adherence and to provide sound guidance around PCI DSS and SOX compliance as well as industry best practices. Everyone's involvement in ensuring that our sensitive information is protected is paramount to the continued success of our company.

Information security must be a team effort involving the participation and support of every RCCL employee who deals with information and information systems. In recognition of the need for teamwork, this policy statement clarifies the responsibilities of users and the steps they must take to help protect RCCL information and information systems. This document describes ways to prevent and respond to a variety of threats to information and information systems including unauthorized access, disclosure, modification, appropriation, destruction, loss, misuse, and denial of use.

1.0 Policy Detail

1.1 Scope

The Information Security policy applies to all personnel who work with data and information systems such as employees, contractors, and business partners. This policy applies to all computer and network systems owned by or administered by RCCL. The policy covers only information handled by computers and networks. Any business partner, vendor, or third party receiving RCCL data or connecting to our network needs to adhere to the Security policies.

1.2 Purpose

The purpose of this document is to define a clear set of information security policies for the operating environment. RCCL relies on information and information systems for fulfilling its business objectives. If important information were disclosed to inappropriate persons, the company could suffer serious losses. The good reputation that RCCL enjoys is also directly linked with the way that it manages both information and information systems. For these and other important business reasons, executive management has initiated and continues to support an information security effort.

1.3 Responsibilities

It is the responsibility of all personnel to review and understand the information security policies. Upon hire and at least annually, all personnel are required to review the Information Security Policy published on the corporate portal under the policy section. RCCL has in place a method electronically or in writing, at least annually, that employees have read and understood the information security policy. There are also actions that are expected from employees such as reporting activities that violate the policies or circumstances that put RCCL network, infrastructure, sensitive information or customer information at risk. RCCL has a formal security awareness program that ensures that all personnel are trained and aware of security principles that protect company assets and information. All employees and contractors must be regularly or continually exposed to information security awareness techniques (e.g., posters, awareness tools, periodic e-mail, warning messages, tips of the day upon accessing an information system, computer/information security day events).

1.3.1 Data Integrity

For the purpose of this document and ease of understanding, IT security will use three categories for understanding ownership responsibilities; at least one of which applies to each employee. These categories are Owner, Custodian, and User. These categories define general responsibilities with respect to information security.

If controls which assure the integrity of information fail, are suspected of failing, or are no longer available, management must be notified of these facts along with supporting documentation whenever evidence arises of such failures, for further detail see the Certified Incident Response Plan (CSIRP) located on the ITLC under Technical Standards. Methods are in place to ensure that all input submitted to production computer systems for processing has been properly authorized.

Information Owners are the department managers, members of the top management team, or their delegates within RCCL who are responsible for the acquisition, development, and maintenance of production applications. All production application system information must have a designated Owner. For each type of information, Owners designate the appropriate level of criticality, define which users will be granted access, and approve requests for various ways in which the information will be utilized.

Custodians are in physical possession of either RCCL information or information that has been entrusted to RCCL. While Information Technology department staff members are Custodians, local system administrators are also Custodians. Whenever information is maintained only on a personal computer, the User is also a Custodian. Custodians are responsible for safeguarding the information, implementing access control systems, and making backups so that critical information will not be lost. Custodians are required to implement, operate, and maintain the security measures defined by information Owners and management's policy and standards. Documents are located on the ITLC under Technical Standards.

Users are responsible for upholding all RCCL policies, procedures, and standards dealing with information security. Questions about the appropriate handling of a specific type of information should be directed to either the Custodian or the Owner of the involved information.

1.4 User Access

Access to information in the possession of, or under the control of RCCL must be provided based on the need to know and only to people who have a legitimate business need for the information. To implement the need-to-know concept, RCCL has adopted a stringent User access request and approval process approved and reviewed by the appropriate Owners. When an employee changes job function, transfers departments, receives a promotion and takes a leave of absence, or is terminated, the supervisor must immediately submit a request based on the standard corporate process. The privileges granted to all employees will be periodically reviewed by information Owners and Custodians to ensure that only those with a current need to know presently have access and there are no segregation of duty risks.

1.4.1 User ID/Passwords

RCCL requires that each employee who accesses the RCCL network have a unique user ID and a private password. These user ID's must be employed to restrict system privileges based on job duties, project responsibilities, and other business activities. Each employee is personally responsible for the usage of his or her user ID and password.

All passwords must have a complexity factor constraint that is system or application enforced. Below are basic password constraints that require adherence:

- User passwords must be at least 9 characters long.
- Administrative passwords must be at least 15 characters long.
- Passwords must not be the same as the User ID.
- Users must not use the same password for multiple IDs and/or multiple systems.
- Passwords must contain at least one non-alphabetic character such as a numeral (0-9) or punctuation character.
- Passwords must be changed every 90 days or at more frequent intervals.
- If an employee suspects that a password has become known, that password must immediately be changed.
- Users must not construct passwords that are identical or substantially similar to the last eight passwords they have previously used.

1.4.2 Password Storage

Passwords must not be stored in readable form in batch files, automatic logon scripts, software macros, terminal function keys, in computers without access control systems, or in other locations where unauthorized persons might discover them. Passwords must not be written down and left in a place where unauthorized persons might discover them.

1.4.3 Sharing Passwords

If employees need to share computer-resident data, they must use electronic mail, groupware databases, or public directories on local area network servers. Although user IDs are shared for electronic mail and other purposes, passwords must never be shared with or revealed to others. System administrators and other technical information systems staff must never ask an employee to reveal their personal password. The only time when a password should be known by another is when it is issued. These temporary passwords must be changed the first time that the authorized user accesses the system. If a user believes that his or her user ID and password are being used by someone else, the user must immediately notify the system administrator for the information system.

1.5 Third Party Data

RCCL internal information must be protected from disclosure to third parties unless it has specifically been designated as public. Third parties may be given access to RCCL internal information only when a demonstrable need to know exists,

when a RCCL non-disclosure agreement has been signed, and when such a disclosure has been expressly authorized by the relevant RCCL information Owner. If sensitive information is lost, is disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties, the information Owner and the Information Security department must be notified immediately.

Unless an employee has been authorized by the information Owner to make public disclosures, all requests for information about RCCL and its business must be referred to Corporate Communications. This policy does not apply to sales and marketing information about RCCL products and services, nor does it pertain to customer technical support calls.

Information about security measures for RCCL computer and network systems is confidential and must not be released to people who are not authorized users of the involved systems unless approved by the Manager of Information Security & Compliance.

Third party software in the possession of RCCL must not be copied unless such copying is consistent with relevant license agreements and either: (a) management has previously approved of such copying, or (b) copies are being made for contingency planning purposes.

1.6 Intellectual Property Rights

While an employee of RCCL, all staff members grant to RCCL exclusive rights to all patents, copyrights, inventions or other intellectual property they originate or develop.

Without specific written exceptions all programs, source code, and documentation generated by or provided by employees, consultants or contractors, for the benefit of RCCL are the property of RCCL. Management must ensure that all users providing such programs, source code or documentation sign a statement to this effect prior to the start date of employment or service agreement.

RCCL has legal ownership of the contents of all data files stores on the computers and network systems as well as all messages transmitted via these systems (see section 2.3 electronic communications). Additionally, RCCL reserves the right to inspect and perform analysis on any network traffic that traverses the RCCL network and reserves the right to access this information without prior notice.

All owners/custodians/users of data that place information in the public data store areas of RCCL servers grant to RCCL the right to edit, copy, republish, and distribute information.

All copyrighted information and software, that RCCL does not have specific approval to store and/or use, must not be stored in RCCL systems or networks. Systems administrators will remove such information and software unless authorization from the rightful owner(s) is provided.

Users must not copy software provided by RCCL to any storage media (removable media, external storage, tape, online or other) or transfer such software to outside parties without written permission from IT Technology and Operations Senior Management.

Exchanges of software and/or data between RCCL and any third party may not proceed unless a written agreement has first been signed. Such an agreement must specify the terms of the exchange as well as the ways in which the software and/or data is to be handled and protected. This policy does not cover release of information designated as public (marketing materials, help wanted postings, etc.)

Users must not disclose software license keys to outside parties without written permission from IT Technology and Operations Senior Management and is not permitted to install unlicensed software on any computer system deemed to be property of RCCL.

2.0 Security

2.1 Physical Security

Physical Security to Control Information Access

Access to every office, computer machine room, and other RCCL work area containing sensitive information must be physically restricted to those with a permissible access. When not in use, sensitive information must always be protected from unauthorized disclosure. When left in an unattended room, sensitive information in paper form must be locked away in appropriate containers. Unattended computer screens must be screen locked, or logged out, to prevent unauthorized access by a passer-by. If a Custodian of such information believes he or she will be away for less than 30 minutes, information in paper form may be left on a desk or in some other readily observed spot only if all doors and windows to

the unattended room are closed and locked. During non-working hours, employees in areas containing sensitive information must lock-up all information. Unless information is in active use by authorized people, desks must be clear and clean during non-working hours to prevent unauthorized access to information.

Access to premises, buildings and areas containing sensitive information should be justified, authorized, logged and monitored. This should apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.

2.2 Network Security

Internal Network Connections

All RCCL computers that store sensitive information and that are permanently or intermittently connected to internal computer networks must have a password-based access control system approved by the Information Security department. Regardless of the network connections, all stand-alone computers handling sensitive information must also employ an approved password-based access control system. Users working with all other types of computers must employ the screen saver passwords that are provided with operating systems, so that after a predetermined period of no activity the screen will go blank until the correct password is again entered. Multi-user systems throughout RCCL must employ automatic log off systems that automatically terminate a user's session after a predetermined period of inactivity.

External Network Connections

All user in-bound session connections to RCCL computers from external networks must be protected with an approved two factor authentication access control system. User passwords are entered and a second authentication is completed with a randomized number sequence each time a log in is attempted.

Network Changes

With the exception of emergency situations, all changes to RCCL computer networks must be documented in a work order request, and approved in advance by the Information Technology department and must align with the procedures and policy governing Change Management. All emergency changes to RCCL networks must be made only by persons who are authorized by the Information Technology department. This process prevents unexpected changes from inadvertently leading to denial of service, unauthorized disclosure of information, and other problems. This process applies not only to employees but also to vendor personnel.

Remote Access

At management's discretion, employees are permitted to work remote with RCCL equipment as needed utilizing remote access through a token authorization process. Permission to telecommute must be granted by each worker's immediate supervisor. Permission to telecommute is dependent on compliance with information security policies and standards. All RCCL users with remote access must comply with all policy and standards accordingly. Activation of remote access technologies for vendors and business partners is available only when needed by vendors and business partners, and immediate deactivation is required after use.

Sensitive Data

RCCL prohibits the copying, moving, storing and sharing of cardholder data as well as additional sensitive and proprietary information. All sensitive data must not be stored on local hard drives or removable electronic media.

Security Compromise Tools

Unless specifically authorized by the Information Security department, RCCL employees must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security. Examples of such tools include those that defeat software copy protection, discover secret passwords, identify security vulnerabilities, or decrypt encrypted files. Without this type of approval, employees are prohibited from using any hardware or software that monitors the traffic on a network or the activity on a computer.

Security Incident Response

RCCL has a plan in place to address varied security incidents as they relate to IT Security, this plan can be found **on the** ITLC under Technical Standards. The purpose of the CSIRP is for guidance on the following:
A. Speed: Helping RCCL personnel quickly and efficiently recover from security incidents.
B. Minimize Risk: Minimizing loss or theft of information or disruption of critical computing services when incidents occur. Minimize legal risk in multiple areas such as personnel, lost personal data, etc.
C. Systematic Process: The need to respond systematically. Following the procedures in this document will increase the likelihood that personnel will carry out all necessary steps to correctly handle an incident.
D. Protect Systems: Protecting systems. Being able to detect and recover from incidents quickly can in many respects, be considered a protection strategy to supplement system and network protection measures.
E. Efficiency: Using resources efficiently. Having both technical and managerial personnel respond to an incident requires a substantial amount of resources. These resources could be devoted to another mission if an incident were to be short lived.

Ending the incident as quickly as possible is, therefore, a high priority so that resources can once again be expended on "normal" operations.

2.3 Internet and Email - Acceptable Use

Internet Access

Employees are provided with Internet access to perform their job duties, but this access may be terminated at any time at the discretion of an employee's supervisor. Internet access is monitored to ensure that employees are not visiting sites unrelated to their jobs, and also to ensure that they continue to be in compliance with security policies.

Employees must take special care to ensure that they do not represent RCCL on Internet discussion groups and in other public forums, unless they have previously received top management authorization to act in this capacity.

Employees are not permitted to place sensitive and confidential RCCL material on any publicly-accessible computer system. If the posting has been approved by both the information owner and the director of the Information Technology department, or is a press release; such information is permissible. Sensitive information, including passwords and credit card numbers, must not be sent across the Internet unless this information is in an encrypted form.

Electronic Mail and Messaging

Every RCCL employee who uses computers in the course of their regular job duties will be granted an e-mail address and related privileges. All RCCL business communications sent by electronic mail or approved messaging system must be sent and received using this company electronic mail address. A personal Internet service provider (ISP) electronic mail account or any other electronic mail address, to include instant messaging, must not be used for RCCL business unless a worker obtains management's approval. Unsolicited electronic mail transmissions to prospects and customers are prohibited. All RCCL employees must refrain from sending credit card numbers, passwords, passport or other sensitive information that might be intercepted. All RCCL staff must additionally employ a standard electronic mail signature that includes their full name, job title, business address, and business telephone number.

2.4 Acceptable Use

Right To Search And Monitor

Management reserves the right to monitor, inspect, or search at any time all RCCL information systems. This examination may take place with or without the consent, presence, or knowledge of the employees. The information systems subject to such examination include, but are not limited to, electronic mail system files, personal computer hard drive files, all electronic communications, printer spool files, fax machine output, desk drawers, and storage areas. All searches of this nature must have prior approval and will be conducted after the approval of the Human Resources executive (Director or Above) has been obtained. Because RCCL computers and networks are provided for business purposes only, employees must have no expectation of privacy associated with the information they store in or send through these information systems. Management retains the right to remove from its information systems any material it views as offensive or potentially illegal. Management reserves the right to revoke the system privileges of any user at any time. Conduct that interferes with the normal and proper operation of RCCL information systems, which adversely affects the ability of others to use these information systems, or that, is harmful or offensive to others is not permitted.

Personal Use

RCCL information systems are intended to be used for business purposes only. Incidental personal use is permissible if the use does not consume more than a trivial amount of resources that could otherwise be used for business purposes, does not interfere with worker productivity, and does not preempt any business activity. Personal use that does not fall into the three categories detailed below requires the advance permission of a department manager:

- Games that are shipped with computer operating systems can be played during scheduled breaks or lunch as long as this activity does not interfere with either worker productivity or intention.
- Games that take the form of separate software packages are prohibited.
- Use of information systems for chain letters, charitable solicitations, political campaign material, religious work, transmission of objectionable material, or any other non-business use is prohibited.

Users must not test, or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by the Information Security department. Incidents involving unapproved system hacking, password guessing, file decryption, bootleg software copying, or similar unauthorized attempts to compromise security measures may be unlawful, and will be considered serious violations of RCCL internal policy. Short-cuts bypassing systems security measures, and pranks and practical jokes involving the compromise of systems security measures are absolutely prohibited.

Software Sources
RCCL computers and networks must not run software that comes from sources other than other RCCL departments, knowledgeable and trusted user groups, well-known systems security authorities, or established computer, network, or commercial software vendors. Software downloaded from shareware, public domain software, and other software from untrusted sources must not be used unless it has been subjected to a rigorous testing regimen approved by the Information Security department.

2.5 Virus, Malware

Computer Virus Screening
All computer users must keep the current versions of approved virus screening software enabled on their computers. Employees must not bypass or turn off the scanning processes that could prevent the transmission of computer viruses. Users must not abort automatic software processes that update virus signatures. Virus screening software must be used to scan all software and data files coming from either third parties or other RCCL groups. This scanning must take place before new data files are opened and before new software is executed.

Computer Virus Eradication
If employees suspect infection by a computer virus, they must immediately stop using the involved computer and call the Help Desk. External disks and other magnetic storage media used with the infected computer must not be used with any other computer until the virus has been successfully eradicated. The infected computer must also be immediately isolated from internal networks as well as disconnected form the RCCL network. Users must not attempt to eradicate viruses themselves. Qualified RCCL staff or consultants must complete this task in a manner that minimizes both data destruction and system downtime.

2.6 Backups

Clean Backups
All personal computer software must be copied prior to its initial usage, and such copies must be stored in a secure location such as a locked file cabinet or offsite. These master copies must not be used for ordinary business activities, but must be reserved for recovery from computer virus infections, hard disk crashes, and other computer problems. For more details on backup standards as required by RCCL, please see *S.2 Backups and Restore Standards on the* ITLC under Technical Standards.

Backup Responsibility
It is RCCL policy if an employee, contractor, consultant or third party vendor uses a non-approved device they must regularly back up the information to a shared folder or drive within the RCCL network. For multi-user computer and communication systems, a system administrator is responsible for making periodic backups. If requested, the Information Technology department must install, or provide technical assistance for the installation of backup hardware and software. All backups containing critical or sensitive information must be stored at an approved off-site location with either physical access controls or encryption. A contingency plan must be prepared for all applications that handle critical production information. It is the responsibility of the information Owner to ensure that this plan is adequately developed, regularly updated, and periodically tested.

2.7 Destruction and Disposal

For detailed information on Destruction and disposal of sensitive information and RCCL equipment, please see the Corporate Policy http://intranet.rccl.com/dept/legal/documents/royal%20caribbean%20cruises%20ltd/main.html
For more detailed information on Server decommissioning and shipboard decommissioning, please visit the ITLC under Technical Standards.

2.8 Mobile Devices

Mobile endpoint security for purposes of this Information Security policy is applicable to all employees, contractors, consultants, and 3rd party vendors. Mobile devices defined but not limited to laptop computers, mobile phones, tablets and smartphones owned by RCCL.

It is the RCCL user's responsibility to protect RCCL capital investments and intellectual property by following the Mobile Device Management (MDM) policy as indicated here.
Ensure mobile endpoint systems are maintained in a secure environment to reduce the threat of loss or theft of the device itself and any sensitive information it may contain. Also, ensure the person allocated to a mobile endpoint system assumes an appropriate level of responsibility for RCCL property. Any RCCL owned endpoint system that is compatible and certified with the RCCL full disk encryption solution must have it installed and operational at all times.

- Take full responsibility for the security of the mobile endpoint and also for the information stored on the device
- Understand that RCCL owned mobile endpoints are the property of RCCL and are intended for business use. Any personal usage of Company equipment must not violate any other Company approved policy or put the asset at risk
- Take all precautions and necessary steps to protect against installation of any malicious or unlicensed software
- Comply with copyright requirements of the software or data used

- Understand that operation of your mobile endpoint in a wireless mode in airports and internet cafes may present additional risks
- Ensure proper care is taken of the mobile endpoint
- Configure mobile endpoints only with RCCL approved software
- Maintain the integrity of virus scanning, encryption, security and management software, do not install additional software or alter the configuration with the intent of blocking security policy and equipment management software
- Take all precautions and necessary steps to prevent use of computer resources for illegal and/or inappropriate activities
- Keep all passwords confidential and never share passwords
- Prohibit unauthorized users form accessing mobile endpoint resources.
- Return obsolete, broken or old RCCL mobile endpoints to IT Customer Care so that they are disposed in a manner that protects collateral information.

2.8.1 Mobile Device Physical Security

- Avoid leaving mobile endpoint systems unattended in public places
- Any sensitive information displayed in the mobile endpoint screen should not be visible to passerby in public places
- Keep mobile endpoints with you and carry as hand luggage while traveling
- Do not perform any unauthorized hardware or software changes to the mobile endpoint. If additional software or hardware is needed, request it from the IT Helpdesk via a Service Request Management (SRM) request
- If you take your mobile device home, be sure to keep it in a safe place
- If you are traveling be sure to lock your mobile device in your hotel safe
- Keep your endpoint in sight when going through airport checkpoints. Many travelers find it helpful to tape their business card to their mobile endpoints. This will help identify your mobile device in airport security
- Do not leave your mobile endpoint device in your vehicle
- Do not use the device in locations that may increase the likelihood of damage.
- Keep food and drinks away from your mobile endpoint
- Always use a padded carry case for your mobile endpoint for additional protection
- If the mobile endpoint device is stolen or lost, it should be reported immediately to your RCCL supervisor

2.8.2 Access Control/Authentication

All mobile endpoint computers' must be password protected and comply with the current password policy. For more information please refer to password detail in section 1.4.

2.8.3 Data Protection

- If required and needed for business use, get an approval to store sensitive data on your mobile endpoint. All sensitive data should be encrypted
- All sensitive data should be backed up on a regular basis in a secure or authorized location
- Whenever possible all sensitive information should be saved on the network servers of the organization
- Anti-virus software needs to be installed and updated regularly
- Store a minimal amount of data on the mobile endpoint

3.0 Exceptions/Violations

The Information Security & Compliance Director acknowledges that under rare circumstances, certain employees will need to employ systems that are not compliant with these policies. All such instances must be approved in writing and in advance by IT Compliance (ITComplianceTeam@rccl.com).

All suspected policy violations, system intrusions, virus infestations, and other conditions that might jeopardize RCCL information or RCCL information systems must be immediately reported to the Information Security department. Any violation of this policy may result in disciplinary action, up to and including termination of employment. RCCL reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

4.0 Policy Administration and Compliance

Compliance Statement - All employees who wish to use RCCL multi-user computer systems must sign a compliance statement annually. A signature on this compliance statement indicates the involved user understands and agrees to adhere to RCCL policies and procedures related to computers and networks, including the instructions contained in this policy.

The below signature(s) represent sound commitment to adhering to the policies detailed above.

Robert Nieves
Manager - IT Security

Date: 12/19/2013

Will Perez
Director - IT Compliance & Security

Date: 12/19/2013

Max Schmidt
VP - IT Operations

Date: 12/19/13

Bill Martin
Chief Information Officer

Date: 12/19/2013

Appendix 1: Data Definitions

Information Classification Guidelines: Notification	Compliance Data Breach Elements	Access Protocol	Transmission	Storage	Logs
Prohibited Information: Notification is required for breaches	Credit Card Data (no storage): • Track Data / Stripe • CVC/CVV2/CID/Pin	NIST-approved encryption is required if information is transmitted through any wireless network, and any non-RCCL wired network. Third party email services are prohibited from transmitting this information.		Cannot store, even if encrypted	Logs need to be enabled and kept for 3 months online and for 1 year offline. Access logging required.
Information Classification Guidelines: Notification	**Compliance Data Breach Elements**	**Access Protocol**	**Transmission**	**Storage**	**Logs**
Information is classified as "Confidential" if (i) it is not considered to be Prohibited or Restricted and is not generally available to the public, or (ii) it is listed as Confidential in the "Classification of Common Data Elements" below	• Staff employment applications • Personnel files • Benefits information • Salary • Personal contact information • Non-public RCI policies and manuals • RCI internal memos and email • Non-public reports • Budgets • Financial information • Employee ID numbers • New build information • Trade Secrets • Mergers • Acquisitions	Access limited to those with a need to know.	NIST-approved encryption is strongly recommended if information is transmitted through any wireless network, and any non-RCI wired network. Third party email services are discouraged for transmitting Confidential information.	Encryption of confidential information is strongly recommended. Level of required protection of confidential information is either pursuant to RCI policy.	Access logging recommended