



INFORMATION AND CYBER SECURITY POLICY

This document is copyright protected in content, presentation, and intellectual origin, except where noted otherwise. You may not modify, remove, augment, add to, publish, transmit, participate in the transfer or sale of, create derivative works from, or in any way exploit any of the elements of this document, in whole or in part without prior written permission from Reliance Home Finance Ltd. © 2018-2019.

Created by:	Harshal Harbak
Reviewed by:	Krishnan Gopalakrishnan Kunal Dikshit Prashant Utreja Lalit Rout
Approved by:	Ravindra Sudhalkar

Distribution List


1. Information Security Risk Management committee (ISRMC)
2. Risk Management Committee (RMC)
3. Information Technology Team
4. Human Resource Team
5. Physical Security Team
6. End Users

Table of Contents

1	General Policies.....	5
1.1	Purpose.....	5
1.2	Scope	5
1.3	Governance	6
1.4	Principles and Objectives	7
1.5	Roles and Responsibilities	8
1.6	Acceptable Usage	18
1.6.1	Acceptable usage of RHFL provided IT assets.....	18
1.6.2	Usage of RHFL Information Systems.....	20
1.6.3	Computer Games	20
1.6.4	Physical Security	21
1.6.5	Handling Confidential Information	21
1.6.6	Storage and Disposal.....	21
1.6.7	Internet User Code of Conduct.....	21
1.6.8	Acceptable usage of social media.....	22
1.6.9	Acceptable usage of personal devices for official purposes.....	23
1.6.10	Acceptable usage of intellectual property.....	24
1.6.11	Acceptable usage of company email facility.....	24
1.6.12	Prevention of misuse of information processing facilities	24
1.7	Risk Management.....	24
1.8	Exceptions	26
1.8.1	Need for exceptions.....	26
1.8.2	Exception grant and risk assessment methodology	26
1.9	Compliance.....	27
2	Security Domain Policy	29
2.1	Data Classification	29
2.1.1	Purpose	29
2.1.2	Scope.....	29
2.1.3	Policy.....	29
2.2	Asset Management	36
2.2.1	Purpose	36
2.2.2	Scope.....	36
2.2.3	Policy.....	37

- 2.3 Access Control 40
 - 2.3.1 Purpose 40
 - 2.3.2 Scope..... 41
 - 2.3.3 Policy 41
- 2.4 Human Resource Security 44
 - 2.4.1 Purpose 44
 - 2.4.2 Scope..... 44
 - 2.4.3 Policy 45
- 2.5 Information Systems acquisition and development 46
 - 2.5.1 Purpose 46
 - 2.5.2 Scope..... 46
 - 2.5.3 Policy 47
- 2.6 Information System Maintenance..... 50
 - 2.6.1 Purpose 50
 - 2.6.2 Scope..... 50
 - 2.6.3 Policy 50
- 2.7 Change Control 53
 - 2.7.1 Purpose 53
 - 2.7.2 Scope..... 54
 - 2.7.3 Policy 54
 - 2.7.4 Change Lifecycle..... 54
- 2.8 Incident and Problem Management 56
 - 2.8.1 Purpose 56
 - 2.8.2 Scope..... 56
 - 2.8.3 Policy 57
- 2.9 Network Security 59
 - 2.9.1 Purpose 59
 - 2.9.2 Scope..... 59
 - 2.9.3 Policy 59
- 2.10 Cryptographic Controls..... 61
 - 2.10.1 Purpose 61
 - 2.10.2 Scope..... 62
 - 2.10.3 Policy 62
- 2.11 Business Continuity Management..... 63
 - 2.11.1 Purpose 63
 - 2.11.2 Scope..... 64

2.11.3	Policy.....	64
2.12	Third party service providers.....	66
2.12.1	Purpose.....	66
2.12.2	Scope.....	66
2.12.3	Policy.....	66
2.13	Physical and environmental security.....	70
2.13.1	Purpose.....	70
2.13.2	Scope.....	70
2.13.3	Policy.....	70
2.14	Monitoring, Logging and Assessment.....	78
2.14.1	Purpose.....	78
2.14.2	Scope.....	78
2.14.3	Policy.....	78
2.15	Cloud Security.....	82
2.15.1	Purpose.....	82
2.15.2	Introduction.....	82
2.15.3	Scope.....	83
2.15.4	Role and Responsibilities.....	84
2.15.5	Policy.....	84
2.15.6	Compliance.....	86
2.15.7	Cloud security lifecycle.....	86
2.15.8	Offboarding of cloud service provider.....	90
2.15.9	Virtualization.....	90
2.15.10	Legal, Regulatory and Contractual Requirements.....	91
2.16	BYOD Security.....	93
2.16.1	Purpose.....	93
2.16.2	Policy Statement.....	94
2.17	Cyber Security.....	97
2.17.1	Purpose.....	97
2.17.2	Scope.....	97
2.17.3	Policy.....	97
3	Glossary.....	102
4	Revision History.....	104

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

1 General Policies

1.1 Purpose

Reliance Home Finance Limited (RHFL) Information and Cyber Security Policy (ICSP) identifies responsibilities and establishes the goals for consistent and appropriate protection of the organization’s Information Assets. Implementing this policy shall reduce risk of accidental or intentional disclosure, modification, destruction, delay, or misuse of Information Assets. This policy enables the Information Security Office to provide direction for implementing, maintaining and improving the security of Information Assets.

Implementing this policy shall also protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology. By implementing this policy, the organization will be able to consistently establish and maintain controls for ensuring confidentiality, integrity and availability of all information assets.

Vision: To provide a user-centric trusted and secure set of resources and environment to employees to conduct business, while ensuring protection of RHFL information assets including customer data.

Mission: Ensuring the security of all RHFL information assets through implementation of up-to-date security mechanisms for prevention and monitoring of threats; governance of information security related activities and awareness of all employees.

1.2 Scope

Information Assets comprise data or information recorded in electronic, printed, written, facsimile or other systems as well as the ‘system’ itself, required for RHFL’s business purpose or operations. Information Assets include business data, system logs, servers, desktops, network equipment, network media, storage media, paper, people etc.

RHFL’s Information and Cyber Security Policy applies to Information Assets throughout their lifecycle, including creation, distribution, transmission, storage and disposal; such as:

- Information Assets in all forms: electronic, printed, written, facsimile, or spoken etc.
- Individuals or organization accessing the information assets like vendors, service providers, distributors, franchisee, customers, service providers, etc.
- Information and Cyber Security Policy shall be supported by Information Security standards, Procedures and implementation guidelines including templates. The Information Security procedures shall be derived from the policy statements and provide the details of necessary actions to achieve the objectives of the policy statements. The templates are derived from the detailed procedures and aim at facilitating the implementation of the Information and Cyber Security Policy and procedures.

1.3 Governance

- **Target Audience**

The target audience for this policy is the employees of RHFL, contractors, and third party service providers who have access to RHFL's Information systems and Information in any form.

The implementation of this policy shall be the responsibility of various departments named in specific sections of this policy such as IT, Administration, Human Resources and the respective Business departments. However, irrespective of specific roles being assigned, all departments must be aware of and comply with this policy.

- **Governing Board**

The Information and Cyber Security Policy (ICSP) of RHFL shall be governed by the Information Security Risk Management Committee (ISRMC) comprising of the Chief Risk Officer (CRO), Chief Technology Officer (CTO), Chief IT Security Officer (CITSO), Chief Information Security Officer (CISO), Chief Security Officer (CSO), Chief People Officer (CPO), Function heads of Operations, Finance, Legal, Compliance. The ISRMC shall be responsible for changes to the policy and approvals thereof. It shall also be responsible to ensure that the policy remains updated at all times and to oversee the implementation of this policy. The ISRMC meeting shall require CISO and at least two members to participate with all members meeting at least once in a year.

ISRMC shall be responsible to conduct Information System Audit of the internal systems and processes at least once in 2 years to assess operational risks faced by the RHFL and the Committee ensures to follow the guidelines issued by Government Authorities/Regulators (GOI/NHB) from time to time.

The implementation and enforcement of the IS policy shall be facilitated by the CISO or Business Information Security Officer (BISO) and governed by the ISRMC.

- **Ownership and interpretation**

The ICSP is owned by the Chief Information Security Officer and shall be maintained by the RHFL "Information Security Team" (hereafter referred to as "IS Team") comprising of the CISO and/or BISO.

CRO will assume the responsibilities of the CISO/BISO in case decision needs to be made in the absence of the CISO/BISO.

- **Review Frequency**

This policy shall be reviewed on an annual basis and if required updated by the CISO/BISO and approved by the ISRMC. The following aspects shall be considered for review of this policy:

- Changes in the regulatory or legal provisions relating to Information Security
- Changes or additions of industry standards
- New Business operations commenced by RHFL in the past one year

- Changes to methods of operating business including changes in the HR policy
- New Channels of business / customer outreach expected to be used by business teams
- New Technologies introduced in the past one year
- Incidents reported within or outside RHFL relating to Information Security.
- Any other considerations as mandated by senior management or board

The renewal of the policy and changes therein shall be notified to all employees of the organization through appropriate means such as emails, intranet notification, annual refresher IS training, educational posters and through the chain of command.

1.4 Principles and Objectives

This policy and supporting procedures shall be based on the following principles and objectives as set below:

- **Information Protection** - Information Assets will be protected at a level commensurate with their value and the risk of loss to RHFL. Protection should stress the confidentiality, integrity, and availability of Information Assets.
- **User Authorization** - All Users must be uniquely identifiable with access permissions specifically and individually authorized based on their business needs. User access methods should stress strong authentication, appropriate authorization and reliable audit-ability.
- **Accountability** - Users and Custodians of RHFL's Information Assets are responsible for the appropriate use, protection and privacy of these assets. All RHFL's system will generate and maintain appropriate audit trails identify Users, and document security-related events and processes.
- **Availability** - Information Assets must be available to support RHFL's business objectives. Appropriate measures must be taken to ensure the timely recovery of all information and access by authorized individuals.
- **Integrity** - Information Assets must be adequately protected to ensure completeness and accuracy. Validation measures will allow detection of inappropriately modified, deleted, or corrupted information.
- **Trust** - Partners, vendors and service providers must demonstrate ability to meet or exceed RHFL's security requirements and justify confidence in their ability to secure RHFL's Information Assets. Trust becomes increasingly important when RHFL's Information Assets are shared with business partners and service providers.
- **Continuity** - Reliance Home Finance must demonstrate the ability to maintain continuity of operations from business and technology perspectives. All information assets and related policies and procedures of RHFL, shall be evaluated from a continuity perspective to support RHFL's business objectives. Partners, vendors and service providers must all demonstrate the ability to meet or exceed RHFL's continuity objectives at all times.

- **Cyber Security Resilience** – To enable effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through appropriate legislative intervention.
- **Regulatory Compliance** – To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem.

1.5 Roles and Responsibilities

The following organization structure would be created and shall remain in existence for the governance, implementation and monitoring of Information Security.



1. Chief Risk Officer (CRO)

The CRO shall:

- Be responsible for the overall risk management functions of the organization which shall include Information Security Risk Management in its purview.
- Obtain regular updates from the CISO/BISO regarding IS related issues / incidents, updates, new initiatives and corrective / preventive actions taken, remain involved in IS related initiatives such as IS awareness and training, IS assessments and escalation of critical IS incidents.
- The CRO, along with the CISO/BISO shall represent information security related event / issues and initiatives at the Risk Management Committee.
- Provide budget for implementing cyber security initiatives and for meeting emergency response arising out of cyber incidents.

2. Chief Technology Officer (CTO)


The CTO shall:

- Be responsible for the security related technology implementation and technology related information security risk management functions of the organization.
- Ensure information security considerations are integrated into planning and budgeting cycles, enterprise architectures, Information Systems design, development and acquisition/system development life cycles.

- Ensure Information Security processes are adhered to and report all incidents of importance to BISO/CISO/CRO
- Shall oversee mitigation of security vulnerabilities identified through internal/external audits or Risk Assessment in timely manner
- Shall be responsible for necessary budgetary requirements to secure & mitigate risk as and when required
- Earmark a specific budget for implementing cyber security initiatives and for meeting emergency response arising out of cyber incidents.

3. Chief Information Security Officer (CISO) and Business Information Security Officer (BISO)

- The CISO/BISO shall report to the CRO for overall Security governance and monitoring of Information Security and shall report to the CTO for Information Security related technology implementations and operations. BISO shall support under guidance of CRO, CTO and CISO in facilitating the IS governance, Security project implementation and monitoring activities and shall be responsible for governance and monitoring of specific focus areas of Information Security as per roles defined by the CRO/CTO.
- The CISO / BISOs shall be responsible for carrying out the following functions:
 - Review IS policy annually
 - Conducting and coordinating both internal and external IS reviews and assessments
 - CISO/BISO shall be responsible for presenting / escalating the budgetary requirements for resources as well as IS reviews to the CRO
 - Be responsible for ensuring reporting of Critical or High severity information and cyber security incidents to relevant regulators.
 - The CISO / BISO shall be responsible for setting IS Standards, Checklist, Guidelines such as:
 - IS guidelines and any supporting templates
 - Standards for Technology Risk Assessments (TRA) for any process / technology change or new technology sourcing
 - Methodology / checklist for performing the TRA and approval matrix based on the results of the TRA
 - Application security and Vendor risk assessment standards, vendor classification standards based on information security requirements and periodicity of risk assessment for each classification of vendors, appointment of a third party or an internal team to conduct risk assessment based on vendor criticality.
 - IS related trainings standards including frequency for IS related trainings for employees / contractors and the IT / IS teams
 - Security testing baselines for conducting Vulnerability Assessment and Penetration Testing of IT systems (infrastructure and applications) including mandating the use of internal and external vendors based on asset classification

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	


- CISO/BISO shall also carry implementation responsibility and would suitably coordinate with concerned CTOs in this regard. It is pertinent to note that Conflict of Interest; if any would need to be avoided and any such matter would be placed before CRO/CTO.
- The CISO shall receive escalations from BISOs on critical / open IS incidents based on their monitoring activities. Also the CISO/BISO shall provide guidance and oversee the tracking and closure of such incidents. The CISO/BISO shall be responsible to highlight the status of critical incidents to ISRMCM.
- The CISO/BISO shall review Standards, Guidelines, Procedures for monitoring, analyzing and reporting of incidents by IS Operations team including the frequency of reporting based on severity of the incidents
- The IS team shall be responsible for and empowered to conduct IS reviews through the following means:
 - Defining the frequency and sample size for a detailed log review of various security solutions managed by IS Operations team
 - Results of reviews conducted by or through the IS team shall be tabled at the ISRMCM, as applicable based on the scope of the review.
 - The CISO / BISO will receive incident reports from the IS Operations Team and the results of Technology Risk Assessment.
 - The CISO / BISO shall be responsible to analyze the TRA results provided to him / her on a periodic basis.
 - Liaison with business for understanding business processes and data classification and reporting GAP's to CISO / CRO/ CTO
 - The CISO / BISO shall provide guidance for closure of all incidents highlighted to them by the IS Operations team and oversee the tracking and closure of incidents. IS team shall highlight any high level / critical / incidents remaining open beyond the defined SLAs to CRO, CTO and ISRMCM.
 - Shall communicate new key risk trends/vulnerabilities to CISO/CTO
 - The BISO shall initiate contact with the relevant investigation authorities to perform detailed forensic analysis on the device once approval has been given by management.
- **SOC responsibilities**
 - Monitoring, reporting security incidents to the CISO/BISO, assisting the CISO/BISO in analysis (i.e. forensics and investigation) and record keeping;
 - First level analysis should be done by SOC team and false positives need to be identified. SOC team needs to report incident to IS or IT team in case they think the event identified as potential incident; depending on the incident type.
 - Tracking and closure of security incidents based on the incident monitoring and management standards set by the IS team;
 - Providing BISOs with required information directly from the source systems, during IS reviews.
 - Define playbooks for various information and cyber security incident scenarios
 - Conduct or participate Cyber security drill as per the requirement

- **Forensics responsibilities**


- BISO shall ensure that external forensic experts are certified as well as competent for the job.
- BISO shall ensure that these external forensic experts are engaged by way of a formal engagement letter with a confidentiality clause. Non-disclosure agreement to be signed with the organization providing forensic services, before the experts are allowed further access.
- BISO shall ensure that the tools and methods used by external forensics experts are acceptable in the court of law. All forensic evidence shall be collected, stored and processed as per the applicable local laws and regulations.
- BISO shall ensure that chain of custody is maintained till closure of the forensic analysis and necessary records are maintained.

4. Chief IT Security Officer (CITSO)/ IT Security Operations

- The CITSO shall report to the CTO and will primarily be responsible for IT related Information Security Operations.
- The implementation and management of the IT Security Operations related tools shall be overseen by CITSO and he/she shall have a responsibility to ensure that any incidents identified through these tools are reported to the CISO / BISO.
- Shall oversee the Technology Risk Assessments (TRAs), and implementation of security related technology solutions and the overall management and maintenance of security solutions.
- Shall coordinate with IT team about Information Security technology areas/issues and ensure action points are addressed to maintain risk level and shall escalate to CTO in case of delay in mitigation.
- Shall be responsible for Risk Mitigation on timely manner and taking residual risk sign off on exceptions
- Shall co-ordinate for addressing resolution for new key risk trends/vulnerabilities as intimated by CISO/BISO
- Receiving and acting upon requests for granting / modification and deactivation of user access on applications / domain, as per the defined access control matrix;
- Conducting periodic user recertification process by providing business teams with access rights register and obtaining approval from them for its validity;
- Obtaining exception approval from the BISO / CISO prior to granting access rights which are not as per the defined access controls matrix;
- Handling and Reporting of access control related incidents to BISO / CISO;
- Providing BISOs with required information directly from the source systems, during IS reviews.
- IT team shall ensure compliance to Information and Cyber Security policy
- IT team shall provide necessary reports to Information Security team where requirement may arise due to internal risk review, incident analysis and investigation or forensics.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- Mapping of RACI Matrix for the areas related to IT
- Access provisioning and de-provisioning as per standard matrix defined by business users
- shall be responsible for performing Technology Risk Assessment (TRA) prior to introduction of a new process or technology or implementing changes to an existing process and technology based on the TRA standard set by the IS team. Based upon the results of the TRA performed, the CISO / BISO shall be notified for approvals required.
- Shall ensure that IT security Operations are run as per the IS Policy and in line with guidelines and standards defined by the IS Team.
- **DLP Responsibilities**
 - Implementation of Data classification standards including data privacy requirements
 - Facilitating implementation of information classification policy and procedures in the DLP tool;
 - Reporting data leakage incidents to BISO / CISO and tracking them to closure;
 - Providing BISOs with required information directly from the source systems, during IS reviews.
 - Implementation and maintenance of DLP across all systems
- **SOC responsibilities**
 - Timely define mitigation plan and address security incidents communicated by SOC team.
 - Reporting status to CISO/BISO with root cause analysis and corrective/preventive action
 - Work with ERT team in case of crises situation to contain and mitigate with depending on the severity defined by IS or ERT team.
 - Provide necessary information to SOC team for incidents analysis and take necessary action to contain risk and mitigate vulnerability.
 - Provide timely status to IS, SOC, ERT team depending on relevance.
 - Provide mitigation for technology related incidents along with Root Cause Analysis and Corrective/Preventive actions for Level 2 and above incidents.
- **Forensics responsibilities**
 - CISO/IT Security Operations person shall isolate the suspected machine from Business/ Unit network and gather audit logs generated by the suspected device.
 - CISO/IT Security Operations person shall store the device in a physically secured and access-controlled location to ensure data integrity is maintained until asset has been handed over to the external forensic expert.
 - CISO/IT Security Operations person shall ensure that routine document destruction is suspended immediately until further notice;
 - CISO/IT Security Operations person shall ensure that necessary information and rights are provided to CISO/BISO and forensic team.
 - CISO/IT Security Operations person shall ensure that necessary records are maintained for all the activities carried during forensic investigations.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- After forensic activity, CITSO/IT Security Operations person shall ensure that earlier access has been restored.

5. Chief Security Officer (CSO)

The Chief Security Officer shall be responsible for:

- Assist the ISRMC and CRO in all aspects of Physical security.
- Ensure physical security processes are adhered to and report all incidents of importance to the CRO.
- Conduct training of the Security staff.
- Run sensitization programs, security week and allied training activities for sensitization of employees.

6. Human Resources

- The HR team shall play a crucial role in Information Security related initiatives of the organization
- HR shall make sure that all new employees are made aware of their infosec related responsibilities by including that as a part of the new joiner induction program. HR shall sensitize new joiners on the importance of complying with the information security related requirements and the repercussions of not doing the same.
- HR shall also make all new joiners sign a declaration / undertaking of having understood and accepting the information security related requirements of the organization and maintain these declarations as a part of the personnel files
- HR shall in conjunction with the Infosec team roll out periodic refresher trainings for all employees / critical vendor personnel and track the completion of these courses
- HR shall conduct / appoint an external agency to conduct background checks for new joiners to ensure that the people with the right background and a healthy perspective join the organization
- HR shall cooperate with the BISO /CISO to drive the organization towards building a pro-infosec environment and also assist them in obtaining relevant certifications related to the same.
- HR shall inform organization and employee role / location / joining and exit related information with IS and IT team for necessary changes in the role of information systems

7. Admin

- The Admin team shall play a crucial role in Information Security related initiatives of the organization
- The Admin team shall ensure that relevant policies / procedures from an information security perspective are appropriately implemented and adhered to such as
 - Physical security policy
 - Clean / clear desk policy
 - Visitor management policy
 - Admin shall work closely with HR and IT to ensure that all physical access to the office premises for separated employees is revoked on or before the last working day


- Admin shall also ensure that appropriate devices such as shredders /filing cabinets secured with lock and key etc are made available so as to ensure the confidentiality of critical data
- Admin shall carryout surprise visits on a periodic basis to ensure that no confidential documents / media is lying on any desks
- Admin shall cooperate with the BISO /CISO to drive the organization towards building a pro-infosec environment and also assist them in obtaining relevant certifications related to the same.

8. ERM (Enterprise Risk Management)

- ERM shall provide the BISO with periodic updates of the status of the current IS Risks and actions needed if any.
- ERM team shall work with IS team for investigations of information security incidents.
- ERM team shall share feedback on business frauds which can be input for Information and Cyber Security Policy / control revision.

9. Functional Head (Line of Business) / Business owner

- Functional head shall be responsible for implementation of Data classification policy. Implementation includes assigning of SPOC's, Data identification, Data classification & Data protection
- Functional head designated SPOC shall liaison with IS Governance team on Data classification governance dashboards
- Functional head designated SPOC shall manage and monitor User ID Onboarding, Transfer and Exit. This user ID can be employee ID's, Vendor ID's, System ID's and Privilege ID's
- Functional head designated SPOC shall ensure periodic review of User ID's with CISO / BISO / CISO / IT / HR
- Have primary responsibility for ensuring that appropriate and adequate security mechanisms are provided in the systems and network infrastructure shared across systems and business units.
- Have primary ownership to comply with specific security policies, which will be applicable for systems development and acquisition.
- Be responsible for maintenance of the various security tools and solutions.
- Be responsible for monitoring of secure status on each system and network within its control. Report on weaknesses or breaches of security to be made to the relevant Business owners or Infrastructure owners and to the CISO, who shall in turn co-ordinate, the incident response.
- Functional teams shall designate a suitable and qualified team member who will be responsible for reporting the incidents & effectiveness of security control to CISO /Information Security Team/ CIO.
- Legal Team — Legal Team is responsible for Engagement with Cyber security police officials, lawyers and Government agencies as required. Necessary details with regards to the incident are provided by information security team.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- Users and Information Owners - System users and data owners are responsible for the application of the policies relating to the systems, data, and other information resources under their care or control. They are also responsible for reporting any suspected cyber security incident to Information Security Team/IT Head.
- Business owners shall hold the primary responsibility for defining the value and classification of assets within their control by participating in the risk management process and undertaking business impact assessment.
- Be responsible for authorizing access and segregation of duties for individual users and groups including Third parties to the information contained within the applications.
- Ensure that appropriate access of administration roles or teams exist for their applications to administer access in accordance with the IS Policy
- Ensure implementation and compliance to Information Security Policies as applicable for their business units.
- Ensure that appropriate access of administration roles or teams exist for their applications to administer access in accordance with the IS Policy.
- Ensure implementation and compliance to Information Security Policies as applicable for their business units.
- Be primarily responsible for risk, data security and access of Third party partners and vendors to whom line of business has been outsourced
- Review the self-assessment of Third parties at defined frequency to whom line of business has been outsourced.
- Be responsible for conducting security assessments and audits of Third party processes / sites)
- Define Information Security requirements for third parties in concurrence with the Information Security team of the organization

10. Internal Audit

- The internal audit and information security functions shall work synergistically: the information security function shall design policies and procedures to protect the organization's information resources, and internal audit shall provide feedback concerning effectiveness of the implementation of these along with suggestions for improvement.
- The Internal audit function shall provide an independent review and analysis of the organization's information security initiatives and objective assurance to the board and executive management on how effectively the organization assesses and manages its risks, including the effectiveness the IT Security Operations and Information Security Risk management structure and roles.
- The Internal audit function shall keep the audit committee apprised of emerging risks and effective ways to address them and it shall identify weaknesses in policies and controls in place to mitigate these risks.
- Internal Audit plan of the organization shall have a separate IS audit plan covering IT/Technology infrastructure and applications. The audit plan and the reports shall be presented to the Audit Committee of the Board


- All instances of non-compliance related to Information security shall be communicated and discussed with relevant line management and CISO.
- The Internal audit function shall carry out independent assessments reviewing the following aspects of Information Security:
 - Key information security risks faced by the organization and policies put in place to defend against them
 - Effectiveness of the IT Security Operations and Information Security Risk management structure and roles
 - Controls put in place by the management to comply with the policies
 - Whether existing controls are being used by the functional managers
 - Effectiveness of operation of the controls in operations

11. Emergency Response Team (ERT)

- ERT shall be formed with presence of IS team, IT team, Admin team, HR team, Legal team, Finance team, Corporate communication team depending on the type of incident.
- ERT capability shall be established so that the organization is ready to respond to incidents and prevent future incidents by ensuring systems, networks and applications are adequately secured.
- Processes shall be in place to ensure proper containment of the security incident and reduce the extent of business impact caused.
- After the incident has been contained, eradication shall be performed to eliminate components of the incident (such as deleting malicious code and disabling breached user accounts).
- Necessary containment, mitigation action plan to be defined, tracked and reported during incidence response.
- Establish a mechanism for sharing information, for identifying and responding to cyber security incidents and for cooperation in restoration efforts.
- A root cause analysis of the security incident shall be carried out to identify what went wrong and identify where to focus security improvements.
- Post eradication, recovery shall be performed to restore the compromised system to a secure operational state and take necessary action to prevent similar incident in future.
- Team shall provide timely status to relevant stake holders till closure of the incident.
- Based on the classification of the security incident artifacts must be collected by skilled forensic professionals.
- Reported and documented security incidents must be used for analysis and statistics to recognize possible gaps within the RHFL environment and to improve the efficiency of incident response.

12. Crisis Manager (CM)

- Crisis Manager shall identify whether the reported security event is the crises scenario.
- Single point of contact for Emergency Response Team
- Assign detailed responsibilities and action steps to manage cyber crisis
- Produce reports/updates for governance committee

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- Identify the active risks along with the threat vectors related to cyber crisis
- Based on the identified risks determine immediate actions in coordination with Emergency Response Team
- Support response and investigation activities related to the cyber crisis
- Manage and coordinate crisis management activities in their respective departments
- Review regulatory impact and compliance obligations in case of a cyber crisis
- Provides legal and regulatory guidance throughout the lifecycle of crisis management
- Diagnose cyber crisis to identify potential legal or HR actions to be taken
- Review regulatory impact and compliance obligations in case of a cyber crisis
- Notify customers in case of crisis affecting customer information
- Coordinate communication of cyber crisis to relevant internal and external authorities

13. ISRMC

- The Committee shall refer to the RMC on any matters related to Information Security Risk Management that come to its attention that are relevant for the RMC
- Committee shall also discuss on Information Security Calendar
- The CISO/BISO shall represent the IS Governance related areas at the ISRMC while the CITSO shall represent the IT Security Operations related areas at the ISRMC
- The ISRMC shall obtain periodic inputs from the Information Security Monitoring Committee which shall include list of security incidents – root cause for the same as well as remediation actions taken.
- The ISRMC shall also receive information regarding new initiatives proposed and the evaluation of the same performed from an Information security perspective by the CISO / CITSO / BISO
- The Committee shall provide relevant periodic assurances to the RMC
- The Committee shall monitor and provide recommendations to the RMC on the organization's Information Security risk profile, appetite and ensure that an appropriate level of internal controls inline with its risk appetite and oversees the identification, management and reporting of Information Security risks to the appropriate Committees.

14. RMC

- The RMC shall receive periodic inputs on matters related to Information Security Risk from the ISRMC.
- At the discretion of the members of the Committee matters considered to be of major importance shall be referred to the Board for its attention.
- The Committee shall monitor and provide recommendations to the Board on the organization's risk profile, appetite and ensure that an appropriate level of internal controls inline with its risk appetite and oversees the identification, management and reporting of risks to the appropriate Committees.
- The committee shall have the responsibility to provide appropriate resources, budgetary approval and direction to the ISRMC from time to time.


15. Board of Directors

- Board shall receive periodic inputs on matters related to Information Security Risk from the RMC.
- Board shall provide guidance to RMC and Information Security team for addressing risk related to Information and Cyber security
- Board shall have the responsibility to provide appropriate resources, budgetary approval and direction to the RMC from time to time.

1.6 Acceptable Usage**1.6.1 Acceptable usage of RHFL provided IT assets**

RHFL shall ensure that the employees, contractors and third parties follow the guidelines for the acceptable use of all the information assets provided by RHFL. Assets shall be used for business purposes and may not be used for carrying out activities which are unlawful in nature including but not limited to hacking, cyber-theft, identity-theft, piracy and pornography.

- **Desktops and Laptop**
 - Confidential data shall not be stored on laptops or desktops. In events where confidential or restricted data needs to be stored on laptops, the data on laptop hard disks should be kept encrypted using at least 128 bit encryption application. All confidential data being copied to removable media should be encrypted. Laptops shall not be left unattended.
 - The folders or disk drives in individual PC's or laptops shall not be shared unless authorized.
 - The virus definition files on all desktops and laptops shall be kept updated.
 - Users shall return the desktop/laptop & all related IT accessories to IT/ HR department/Designated person only before their release/ leaving the organization and shall not handover it to anyone else within the department/organization.
 - In case of laptop theft /loss, user needs to file FIR with the police and submit FIR copy to IT team for the insurance claim.
- **Telephone / Mobile**
 - Staff shall not reveal sensitive or classified information over the telephone unless the telephone lines have been specifically secured for this purpose.
 - Staff shall not enter into the conversation or reveal any information to over the telephone where the identity of the caller cannot be determined.
 - Staff shall not discuss confidential matters or reveal confidential / classified information in public places and / or outside RHFL premises.
- **Fax Machines**
 - Sensitive or confidential information shall be faxed only when necessary.
 - Users who are responsible for receiving confidential fax messages shall co-ordinate with the sender to ensure that they are present at FAX machine at the time of delivery.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- **Modem / Data Cards / Internet Dongles**
 - User's shall be responsible for physical custody of Data card and shall ensure utmost care from theft, misuse and mishandling
 - User's shall return Data card to IT/HR if not in use or during exit process
 - Misplace / Theft of data card shall be reported promptly to HR/IT
 - Modems shall not be attached to workstations without authorisation from Information Security Group.
 - Laptop users shall not connect to the public domain using the internal modems in laptops and be connected to RHFL network at the same time.
- **Printer**
 - All printouts, faxes, photocopies and scanned documents containing internal, restricted or confidential information must be collected immediately from the printers, fax machines or photocopier respectively
 - Printers shall only be used for official purpose.
- **Password Standards**
 - Passwords provide a means of validating a user's identity and thus to establish access rights to information processing facilities or services. All users should:
 - Keep their passwords confidential and change at regular interval as per password policy section
 - Do not share individual user ID's/ passwords.
 - Select quality passwords with a minimum length of 8 characters, which are difficult to guess and is complex by nature (contain one numeric and one special character).
 - Password history to be configured and all users shall not be able to use previous passwords
 - Maximum Password age to be configured and all user's shall be prompted for password change before expiry
 - Avoid keeping a paper record of passwords, unless this can be stored securely;
 - Do not include passwords in any automated log-on process, e.g. stored in a macro or function key
 - Successive login failures will result in a user's account being locked; the user shall contact IT support Engineers for getting the account unlocked.
 - Change passwords whenever there is any indication of possible system or password compromise
- **Virus Protection**
 - Users shall not open any files attached to an email from an unknown, suspicious or untrustworthy source.
 - Users shall delete chain/junk emails and not forward or reply to any of the chain/junk mails. These types of email are considered Spam, which is unsolicited and intrusive.

- Users shall exercise caution when downloading files from the Internet and should download only from a legitimate and reputable source. Verify that an anti-virus program checks the files on the download site.

1.6.2 Usage of RHFL Information Systems

- Users shall use RHFL information resources for business purposes only, for which they have been authorized.
- Users shall avoid accessing rogue areas on the company networks for which they do not have a valid business need.
- Usages of RHFL information systems shall not be used to store, process, download, or transmit data that can be construed as biased (politically, religiously, racially, ethnically, etc.) or supportive of harassment.
- Receiving, printing, transmitting, or otherwise disseminating proprietary data, company secrets, or other confidential information in violation of company policy or proprietary agreements shall be considered as violation to the policy.
- Users shall not be downloading inappropriate material such as picture files, music files, or video files for personal use.
- Users shall terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver;
- Users shall follow a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities in order to reduce the risks of unauthorized access, loss of, and damage to information during and outside normal working hours.
- Introduction of Unauthorized Copies Of Licensed Software & Hardware
 - Users shall not introduce unauthorized copies of licensed software & hardware (piracy/copyright & patent infringement) to RHFL information resources and the copying of such material is not allowed.
 - The storage, processing, or transmittal of unauthorized copies of licensed software & hardware (piracy/copyright & patent infringement), by RHFL personnel associates is not allowed.
- Introduction of Open-source, Freeware and Shareware Applications
 - Introduction of Open-source, Freeware and Shareware Applications whether downloaded from the Internet or obtained through any other media to RHFL information systems shall be subject to a formal security assessment and approval process by Information Security team. Open-source system shall be used for monitoring and reviewing any production systems after security assessment and approval of the same by the BISO.

1.6.3 Computer Games

- Users shall not install any computer games in RHFL information resources and play within office premises

1.6.4 Physical Security

- Users shall not enter into RHFL premise without ID badges and they shall always display their ID badges with in RHFL premise.
- Users shall not take in or out any equipment from RHFL premise, without authorization other than Laptop and tablets provided by RHFL.
- Under NO circumstances, consultants or other Visitors personal / official devices be connected to RHFL network until right approvals has been sought.

1.6.5 Handling Confidential Information

- Confidential/restricted information transmitted over any communication network shall be sent in an encrypted form
- Confidential information not being actively used, when stored or transported in computer-readable storage media (such as magnetic tapes, CDs, USBs), shall be in encrypted form.
- Sharing of MIS or any kind of reports containing confidential (customer / company related) data on emails, USB or CD's shall follow "Data Classification Policy". Any exceptions Information Security team.
- Data sent to third parties or shared with them shall be encrypted.

1.6.6 Storage and Disposal

- Physical records shall be secured by storing them securely, shredding them when not needed.

1.6.7 Internet User Code of Conduct

- **Internet "inappropriate" use**
 - The use or attempt to initiate such activities using RHFL's computing facilities or equipment leading to abusive, unethical or "inappropriate" use of the Internet is considered grounds for disciplinary, legal and/or punitive actions as per Information and Cyber Security Policy. Implied restrictions on Internet
 - Users using RHFL's computers on discovering that they have connected with a web site that contains potentially offensive material shall immediately disconnect from that site.
 - Users shall be made aware that RHFL accepts no liability for the exposure to offensive material that they may access via the Internet.
 - The ability to connect with a specific web site does not in itself imply that users of RHFL's systems are permitted to visit that site.
 - Use of online gaming websites, downloading of songs, storing of songs on shared drive or local system is prohibited.

1.6.8 Acceptable usage of social media

- **Usage of social media by corporate employees for corporate purposes**

- Those authorized to use social media in the workplace have a responsibility to use the tools in an appropriate manner as mentioned in “Social Media Policy”. For more details please refer Social Media Guidelines.
- Employees shall not use any social media tool for business unless they have received appropriate training recommended or approved by corporate communication team
- Unless previously authorized in writing by an appropriate authority as per “Social Media Policy”, the employees are categorically restricted, during office hours & while on duty or while using the office network or the officially provisioned means of communications.
- Employees shall refrain from disseminating any unverified and confidential information related to RHFL on any Blogs/Chat forums/Discussion forums/Messenger sites/Social networking sites.
- Any information received, accessed or obtained by an employee, either in his/her official mail/personal mail/Media Forums or in any other manner, if proposed to be disseminated or shared in any Media Forum, shall be forwarded to the Company’s Compliance team and corporate communication team for prior approval.
- Media Forum shall not be used to report a service fault or to make a complaint
- All online participation must be attributable and transparent i.e. no anonymous posts or posts using a pseudonym


- **Guidelines for usage of social media by employees for personal purposes**

- RHFL’s reputation is closely linked to the behavior of its employees, and everything published reflects on how RHFL is perceived. Social media shall be used in a way that adds value to the RHFL’s business. For more details please refer Social Media Guidelines.
- Considering the following points may help avoid any conflict between personal use of social media and an employee’s employment at RHFL:
 - When subscribing to or posting information to an online/internet networking service, RHFL personnel must not use their RHFL email address or other RHFL details, unless use is required for genuine business and professional purposes.
 - Any personal internet posting or communication (for example blogs, messages, posting or tweets) of any sort shall be identified as your own individual and personal interactions. These personal interactions shall not in any way be assigned to RHFL or written in such a way that they could be interpreted as corporate RHFL communications, unless explicitly approved by compliance team, corporate communication team or marketing Team.
 - Any personal internet posting or communication which implies that you work for RHFL must include a simple and visible disclaimer such as “The postings on this service are my own personal views and not those of RHFL and are not intended to be interpreted as such”.

- The personal image projected in social media affects an individual’s reputation and may affect the reputation of RHFL. No form of critique or comment on RHFL or its business shall be made on personal websites or social networking platforms.
- When using social media for personal purposes, employees must not imply they are speaking for RHFL. The use of the official e-mail address, official logos or other identification shall be avoided and it shall be made clear that what is said is not representative of the views and opinions of RHFL.
- Employees shall comply with other RHFL policies when using social media. For example, staff shall be careful not to breach RHFL’s Confidentiality and Information Security, or the Employee Code of Conduct. If in doubt, don’t post it.
- Staff shall be mindful of their privacy settings.
- Employees shall be aware that if they break the law using social media (for example by posting something defamatory), they will be personally responsible.
- Employees shall be aware that by revealing certain details they might be more vulnerable to identity theft.
- The BISO shall conduct training and awareness programs along with corporate communication team to educate the employees about information security related social media guidelines and existence and usage of enterprise DLP tools by Reliance Home Finance.

1.6.9 Acceptable usage of personal devices for official purposes

- In the event of a personal device belonging to an employee, contractor or third party being used to access RHFL’s information, the following shall apply:
 - Access to RHFL’s information using personal devices shall be subject to adherence to RHFL’s IS policy
 - RHFL may access corporate information, applications, and data stored on personal devices while they are enrolled with the Company
 - RHFL has rights to monitor the device while it is connected to company’s IT environment
 - The employee is responsible for protection of all forms of RHFL’s data that is contained in the personal device
 - In any of the following events, RHFL has the authority to remotely wipe Company data on personal devices (and personal data if requested by employees)
 - Loss/ misplacement of device
 - Replacement or disposal of device
 - If employment is terminated by either party
 - In case of violation of the company’s policy, RHFL may take any or all of the following steps, among others:
 - Disconnection of service and corporate access of the device to be revoked
 - Discontinuation of reimbursements related to personal device
 - Surrender of device and/or remote wiping of the device

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- Measures as decided by the Management

1.6.10 Acceptable usage of intellectual property

- Procedures shall be put in place to ensure that terms and conditions and license requirements of the copyrighted software or any other proprietary information used within RHFL are complied with.

1.6.11 Acceptable usage of company email facility

- Company email facility must be used as per guidelines laid by Reliance Home Finance Team. Disciplinary action may be taken for any wilful violation to the guidelines. Please refer “Email Usage Guideline” for more details.

1.6.12 Prevention of misuse of information processing facilities


- Information processing facilities must be used as per policies detailed in the Information and Cyber Security Policy, User Polices and guidelines. Disciplinary action may be taken for any wilful violation to the policy.

1.7 Risk Management

Information Security Risk Management is necessary in order to maintain RHFL’s competitive advantage via positive image and reputation as a secure, discreet, and trustworthy organization. Risk must be managed to prevent monetary loss, loss of customer confidence, and/or loss of operating licenses. Risk Management has the following objectives:

- To analyze and recommend particular configurations of technology corresponding with levels of information risk acceptable to the business.
- To identify and oversee the development of new security technology enabling new business processes without increasing unacceptable security risk.
- To monitor deployed information assets to ensure that they maintain the recommended security configurations consistent with the accepted level of risk.
- To educate RHFL’s employees, partners and management on the information security risk present in their areas of responsibility.
- To analyze and manage information security risks incurred by any given business area in such a way that it does not expose further RHFL to unacceptable levels of risk
- Risk roles shall exercise segregation of duties

The Information Security risks associated with business processes and systems changes will be assessed for the impact and the cost of implementing various controls to mitigate them. Decisions with respect of acceptance of risks and implementation of controls will be made at an appropriate level in the organization as defined in the process below:

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	


- **Technology Risk Assessment Process**

- The Information Security team shall define risk assessment templates and/or checklists for assessment of various types of information assets and Information Security processes.
- The technology risk assessment template shall be designed such that the output of the assessment reflects the following:
 - Information security risks resulting from introduction of the new technology / process or change.
 - Controls for mitigation of the risks identified.
 - Residual risks post identification of controls classified as per the nature of the residual risks viz. Financial, Operational, Regulatory or technology
- Based on the nature of residual risks appropriate approvals shall be taken from the risk owners as defined below:
 - Financial – CFO
 - Operational – COO and Business Process Owner
 - Enterprise / Information Security – BISO/CISO/CRO
 - Reputation – CRO/CMO
 - Regulatory – CRO
 - Technology - CTO
- All risk assessment templates / checklists shall be reviewed by the IS team for the appropriateness of the assessments.
- The Information Security Team shall also review the signed off risks on an periodic basis to identify appropriate solutions being available in consultation with the risk owners

- **Information Security Risk Management Process:**

The information security risk management process shall be iterative in nature, involving the following steps:

- Analyzing the planned application of technology to the business requirements.
- Identifying the corresponding information security risks using applicable Risk Assessment (RA) standards.
- Together with the relevant business and support areas, analyzing the cost and effort of implementing security controls to target the appropriate risk level.
- Implementing security technologies, controls and processes to properly mitigate information security risk to the agreed upon level.
- Where necessary, initiating objective measurements and tests of the security controls as implemented.
- Monitoring security controls after deployment to ensure their stability and adequacy.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

1.8 Exceptions

1.8.1 Need for exceptions

When situations that require an exception to the Information Security Policies arise, the decision whether to accept the risk of not following the applicable Technology Risk Assessment standard must be made at senior management level. Prior to such a decision, the Risk Assessment shall be performed and appropriate approvals need to be obtained as mentioned in “Risk Management” section. The purpose of such a process is to ensure adequate analysis and conscious acceptance of the risk represented by non-compliance with a policy.

1.8.2 Exception grant and risk assessment methodology

- **Risk Assessment Process**


A risk assessment must be completed and approved to support any decision not to comply with any requirement of RHFL’s Information and Cyber Security Policy. All policy exceptions must be fully documented, approved by as mentioned in “Risk Management” section, and retained by the Information Security Team as long as the exception exists. The documentation must be completed and maintained by the Information Security Team and must address:

- The value and sensitivity of the information asset at risk, including the business consequences of its disclosure, destruction, modification, delay, or misuse.
- The policy (or policies) to which the exception applies.
- A description of the risk and exposure that results from non-compliance
- Acceptance of the risks identified
- The business reason for non-compliance.
- Any compensating controls that will reduce the risk to an acceptable level.
- Any actions, that will lead to compliance, and a schedule to implement those actions

- **Executive Approval**

Any changes to the Information Security environment of RHFL, which expose the organization towards inordinate risks which cannot be mitigated by putting in place appropriate controls, shall be approved by Information Security team as defined in various sections of this policy. Executive approval signifies:

- Understanding of the risk factors involved in the decision not to comply with policy or standards.
- Concurrence with the decision to accept resulting risk.
- If corrective action is planned, the projected time frame for correction shall be identified and actions shall be tracked to closure.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

1.9 Compliance

Management is responsible for ensuring compliance and for taking corrective action when security controls are not in accordance with these policies.

All employees and contractors must handle RHFL's Information Assets and technology equipment in a manner consistent with RHFL's Information Security Policies and with applicable Employee Policies and Rules of Conduct.

- **Compliance to applicable legislations**
All relevant statutory, regulatory and contractual requirements, pertaining to each business shall be defined explicitly and documented for each of RHFL's information systems. RHFL shall ensure compliance to each of the Laws and Acts relevant to its operations wherever applicable. These will include but not limited to Information Technology (IT) Act, National Housing Bank (NHB) Guidelines or any other regulatory, laws or acts as applicable.
- RHFL shall ensure that the Information System Audit of the internal systems and processes is to be conducted at least once in two years separately through a Certified Information System Auditor (CISA) to assess operational risks faced by the Company in compliance with the National Housing Bank circular NHB(ND)/DRS/REG/MC-07/2017 dated July 1, 2017 and the provisions of the Housing Finance Companies – Corporate Governance (NHB) Directions, 2016.
- **Intellectual Property Rights (IPR)**
Procedures shall be put in place to ensure that terms and conditions and license requirements for the copyrighted software or any other proprietary information used within RHFL are compiled with
- **Punitive actions**
Compliance with Information and Cyber Security Policy (ICSP) is mandatory. If an individual violates the provisions in the Information and Cyber Security Policy, either by negligence or intent, RHFL reserves the right to take appropriate measures such as disciplinary action, dismissal, legal prosecution, claims for compensatory damages, or other as appropriate.

Any non-compliance to the Information and Cyber Security Policy, shall be brought to the notice of the CISO/BISO, either through the incident management process or through a proactive report from an employee or external agency (empowered to conduct an IS review), shall be evaluated by the CISO and consulted CRO/Risk Containment Unit/ Fraud Prevention Unit depending of the type of violation and shall be communicated to HR department for necessary action as detailed below.

Violations shall be categorized into three levels as follows -

- **High Severity:** Non-compliance, which can compromise the security of confidential data or result into significant financial loss, regulatory non-compliance or legal implications for the organization, shall be classified as High Severity violation.
- **Medium Severity:** Non-compliance, which can compromise the security of restricted data or result into reputation loss, operational impact or expose the organization to technology risks, shall be classified as Medium Severity violation.
- **Low Severity:** Non-compliance or incidents of substandard performance, which can compromise the security of internal data or result into minor operational impact, shall be classified as Low Severity violation.

For repeated incidents by the same individual, caused due to the same nature of violation, the severity of incidents shall escalate as defined below:

Number of Repetitions	Severity Category		
	High Severity	Medium Severity	Low Severity
3	High	Medium	Low
4	High	High	Medium
5	High	High	High

Punitive actions for each category of the violation shall be as given below:

Severity Category	Possible Punitive Action
High	Termination of Employment / Cancellation of Contract / Prosecution
Medium	Written Warning / Suspension / Demotion
Low	Initial Discussion / Oral Warning


For repeated but relatively minor incidents of substandard performance, misconduct, or rule violations, corrective counseling may be adopted followed by:

- Initial discussion
- Oral Warning

Prior to any disciplinary action that affects an individual's pay including suspension, demotion, termination and prosecution, the CISO/BISO shall notify the CRO and an investigation shall be required to be performed by a team designated by the CRO. The investigation team shall determine the impact of the non-compliance on the organization considering the following aspects:

- Financial Loss to the organization
- Reputational loss to the organization
- Regulatory or legal implications
- Operational impact and resulting measure of financial impact to the organization
- Technology risks such as obsolescence or lack of appropriate support
- Whether the non-compliance is a result of willful misconduct or resulting from lack of awareness of the policy

Based on the above analysis, the investigation team shall make a diagnosis of the problem to determine appropriate disciplinary action.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

2 Security Domain Policy

2.1 Data Classification

2.1.1 Purpose

To provide a framework for information owners to determine and classify the sensitivity levels for the information that RHFL uses, processes, and stores.

The unauthorized disclosure, modification, accidental or intentional damage, or loss of sensitive RHFL information could constitute a violation of laws and/or regulations, may negatively affect customers, and impact RHFL's image as well as competitiveness in the market. Hence data needs to be classified based on its criticality to enable implementation of security controls commensurate with its criticality.

2.1.2 Scope

This policy applies to information systems, including IT applications, IT infrastructure and physical information channels, and the information assets that RHFL uses, process, and stores using those systems. It also applies to the business processes and procedures at RHFL regarding data processing.

This policy applies to all individuals handling data as well as technology systems where RHFL's information assets are stored or processed.

Technology systems, communications and network connections include but are not limited to network devices such as routers and firewalls, storage devices such as USB drives, and disk drives, servers and mainframes, operating systems, databases and applications.

All Business Units or Departments shall comply with this Information and Cyber Security Policy.

"Data" means a representation of information, knowledge, facts, concepts, or instructions, which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed, or has been processed in a computer system or computer network, and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.


"Electronic Form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device; includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche; (Amended vide ITAA-2008)

"Electronic Record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche; "Information

2.1.3 Policy

The Information Owner shall only classify information assets within their purview using one of the following four classification levels:

- Public
- For internal use only

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- Restricted
- Confidential

Classification levels shall be defined based on the information asset’s relative risk, value, and sensitivity.

Further, any personally identifiable information (PII), shall be identified and classified as PII in addition to being classified as per above data classification policy. RHFL shall employ reasonable and appropriate safeguards to protect the integrity, confidentiality, and security of all PII.

Any breach of this policy shall be considered as an incident and shall be treated as per the incident management policy.

2.1.3.1 Data Ownership

All information assets within RHFL shall have a designated owner. Managers responsible for business processes that utilize information assets are considered the owners of that information. Information owners may delegate ownership of some or all of their information systems to other persons; however, owners shall remain accountable and oversee that delegated owners fulfill their responsibilities.

2.1.3.2 Responsibility of Data Owners

Information owners are responsible for the security of the information systems that support their business processes, as well the information transmitted, processed, or stored by them, either in electronic or physical form. The business owner is ultimately responsible for adequate security of their information assets that reside in those systems.


2.1.3.3 Data Classification Process

Information owners shall ensure that the information assets for which they are responsible are assigned a classification rating that properly indicates its business value and criticality to the organization. Owners shall review the assigned classification label at least every two years to address changed business value and risks, or as required by laws and regulations that impact RHFL.

2.1.3.4 Data Classification Ratings

Information owners are responsible for classifying information into one of the four classification levels based on its level of sensitivity. When in doubt, the highest level of classification shall be applied.


- **Confidential:** Personal or company information that is classified as highly sensitive by senior management or laws and regulations that impact RHFL. Normally this concerns personally identifiable information (PII) about customers, business partners such as agents, distributors, suppliers etc., or employees, or information that is of vital or strategic importance to the success of the organization (e.g., financial statements) and can provide it with a significant competitive edge (e.g., new product designs). Unauthorized disclosure of confidential information could substantially impact RHFL, its brand and/or reputation, and its customers.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	


- **Restricted:** Will constitute of Information assets, which, if disclosed, would result in significant adverse impact, embarrassment, financial penalties, loss of stakeholder confidence and compliance penalties.
- **Internal Use only:** Will constitute of Information that is not intended for use by the public. This can include information posted on company intranet for employee use, such as phone directories or the Employee Handbook. Unauthorized disclosure of Internal Use Only information could moderately impact RHFL, its brand and/or reputation, and its customers.
- **Public:** Will constitute of Information that is approved for release to the public by RHFL’s senior management. Examples include information that is available from public or government sources, advertising, or information posted on official; website. Disclosure of Public information will likely have little or no impact on RHFL, its brand and/or reputation, and its customers.
- **Technical Standards:** Technical standards shall be based on the life cycle process defined below in this document. Section 2.1.3.5 ‘Lifecycle Processes’ outlines the specific controls to protect the confidentiality and integrity of RHFL’s information assets.

2.1.3.5 Lifecycle Processes


- **Confidential Information**
 - Labeling Requirements: A label of “CONFIDENTIAL” shall, at a minimum, be legible on every page of the physical or electronic document.
 - i. Any device or object (including portable devices) that contains CONFIDENTIAL information shall be labeled as “CONFIDENTIAL”.
 - ii. Systems that contain CONFIDENTIAL information shall be identified and mentioned in “Asset Library”.
 - iii. Storage repositories that maintain CONFIDENTIAL information shall be known and controls implemented to effectively protect the information.
 - iv. Emails that contain CONFIDENTIAL information shall, at a minimum, contain “CONFIDENTIAL” in the subject line, header, or footer.
 - Storage Requirements
 - i. Storage environments shall require user authentication that can uniquely identify each user or administrator.
 - ii. Storage environments shall be periodically reviewed and audited to help ensure that information is sufficiently secured.
 - iii. Storage environments shall be monitored to help ensure that access control systems are functioning properly.
 - iv. CONFIDENTIAL information shall be stored on company owned or controlled systems or on equivalently secured systems with which RHFL has an approved partnership.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	


- Transfer Requirements
 - i. When CONFIDENTIAL information is transmitted outside of the RHFL network, including the Internet, it shall be sent in encrypted form or via a secured channel. Encryption keys shall be managed and protected by authorized resources as defined in the Cryptographic Security policy.
 - ii. CONFIDENTIAL information entrusted to RHFL by a third party shall be encrypted when sent over external network systems.
 - iii. CONFIDENTIAL designations shall appear on the cover sheet of transmitted documents (i.e., facsimile transmissions).
 - iv. Phone calls, SMS or electronic communications that discuss CONFIDENTIAL information shall be preceded by a statement about the sensitivity of the information involved.
 - v. When distributing CONFIDENTIAL information via physical format (paper, disks, etc.), enclose the information in an envelope labeled “CONFIDENTIAL” even when delivered by hand.
 - vi. Intellectual Property shall not be transmitted without prior authorization from the Information Owner
- Tracking Requirement
 - i. Tracking techniques, systems capabilities, or manual efforts shall indicate who has accessed the CONFIDENTIAL information, from where is it access (e.g. MAC ID, IP address) and when it was accessed.
 - ii. This access shall be audited by the Information Owner and deficiencies corrected in a timely manner.
- Disposal Requirements: CONFIDENTIAL information shall be completely and securely destroyed at the end of its retention period OR at the release of a litigation or audit hold, if such hold extends beyond the retention period.
- **Restricted Information**
 - Labeling Requirements
 - i. A label of “RESTRICTED” shall, at a minimum, be legible on every page of the physical or electronic document. Any device or object that contains RESTRICTED information shall be labeled as “RESTRICTED”.
 - ii. Systems, applications, and databases that contain RESTRICTED information shall provide a legible label of “RESTRICTED” on appropriate output or displays.
 - iii. Storage repositories that maintain RESTRICTED information shall be known to the Information Owner and controls implemented to effectively protect the information (i.e., physical locks, door locks).

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- iv. Communications that contain RESTRICTED information, at a minimum, shall contain a statement that helps ensure the recipient understands the sensitivity of RESTRICTED information and the handling procedures for RESTRICTED information.
- v. Emails that contain RESTRICTED information shall, at a minimum, contain “RESTRICTED” in the subject line, header, or footer
- o Storage Requirements
 - i. Portable media, hard copy documents, diskettes, or tapes containing RESTRICTED information shall be secured at all times (either through lock and key or electronic authorization processes) and shall be kept under direct control by authorized personnel.
 - ii. Storage environments shall require user authentication wherever possible that can uniquely identify each user or administrator, even for portable electronic devices.
 - iii. RESTRICTED information shall be stored on company owned or controlled systems, or on equivalently secured systems with which RHFL has an approved partnership.
 - iv. Storage environments shall be periodically reviewed and audited to help ensure they are sufficiently secured.
 - v. Storage environments shall be monitored to help ensure that access control systems are functioning properly.
 - vi. Hard copy RESTRICTED information shall be stored in a secured container, such as a locked cabinet or locked desk when not in use or when not under direct visual supervision.
- o Transfer Requirements
 - i. When RESTRICTED information is transmitted electronically outside of the RHFL network, including the Internet, it shall be sent over a secured channel or in encrypted form.
 - ii. Encryption keys shall be managed and protected by authorized resources as defined in the Cryptographic Security policy.
 - iii. RESTRICTED information transmitted electronically shall be accompanied by a caution to the recipient as to how the RESTRICTED information shall be handled and protected.
 - iv. When transmitting RESTRICTED information via physical format (paper, disks, etc.), enclose the RESTRICTED information within double envelopes. The internal envelope shall be labeled “RESTRICTED”. The external envelope shall have no special markings and shall be delivered by hand or as appropriate.
 - v. RESTRICTED designations shall appear on the cover sheet of transmitted documents (ex. facsimile transmissions).

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- vi. RESTRICTED information shall not be discussed with anyone, including associates, contractors, or other third parties who do not have a “need-to-know” and have not been expressly authorized by the Information Owner
- vii. RESTRICTED information shall not be verbally communicated within insecure facilities. Individuals shall ensure that there are no unauthorized persons within earshot before conversation begins.
- o Tracking Requirements
 - i. Tracking techniques, systems capabilities, or manual efforts shall indicate who has accessed the RESTRICTED information, from where is it accessed (e.g. MAC ID, IP address) and when it was accessed.
 - ii. This access shall be audited by the Information Owner and deficiencies corrected in a timely manner
- o Disposal Requirements
 - i. RESTRICTED information and all related copies and back-ups shall be completely and securely destroyed at the end of its retention period OR at the release of a litigation or audit hold, if such hold extends beyond the retention period
- **Internal Use only information**
 - o Labeling Requirements
 - i. INTERNAL USE ONLY information does not have any specific labeling requirements. However, if information or an information source is not labeled, at a minimum it shall be treated as INTERNAL USE ONLY.
 - ii. A label of “INTERNAL USE ONLY” shall be legible on the first page of the file, document, or on the front of the device.
 - o Storage Requirements
 - i. The storage environment shall require user authentication that can uniquely identify each user who accesses the information.
 - ii. Appropriate controls shall be put in place to ensure that only authorized users get access to “INTERNAL USE ONLY” information.
 - o Transfer Requirements
 - i. 1. Generally, INTERNAL USE ONLY information is only transferred to and from those parties requiring use of its content. It is the responsibility of the Information Owner to define and communicate procedures and controls governing the transfer of INTERNAL USE ONLY information
 - o Disposal Requirements
 - i. INTERNAL USE ONLY information shall be disposed of at the end of its retention period OR at the release of a related litigation or audit hold, if such hold extends beyond the retention period

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- **Public Information**

- Labeling Requirements: No labels required
- Storage Requirements: No specific storage requirements
- Transfer Requirements: No specific transfer requirements
- Disposal Requirements: PUBLIC information shall be disposed of at the end of its retention period OR at the release of a related litigation or audit hold.

2.1.3.6 Data Privacy

Personally Identifiable Information (PII) is information about a person that contains some unique identifier, including but not limited to name or unique identification number, from which the identity of the person can be determined. PII may be further bifurcated into-

- Sensitive Personal Information
- Other Personal Information

- **Identification of Personally Identifiable Information (PII)**


Sensitive personal data or information of a person shall include information collected, received, stored, transmitted or processed by body corporate or intermediary or any person, consisting of:

- Password
- User details as provided at the time of registration or thereafter
- Information related to financial information such as Bank account / credit card / debit card / other payment instrument details of the users
- Physiological and mental health condition
- Medical records and history
- Biometric information
- Information received by body corporate for processing, stored or
- Processed under lawful contract or otherwise
- Call data records

Any PII which is not considered SPI as per the above categorization will be treated as OPI.

- **Collection of PII**

- RHFL corporate or any person on its behalf shall obtain consent of the provider of the information regarding purpose, means and modes of uses before collection of such information
- RHFL corporate or any person on its behalf shall not collect sensitive personal information unless –

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- The information is collected for a lawful purpose connected with a function or activity of the agency
- The collection of the information is necessary for that purpose
- While collecting information directly from the individual concerned, RHFL corporate or any person on its behalf shall take such steps as are, in the circumstances, reasonable to ensure that the individual concerned is aware of –
 - The fact that the information is being collected; and
 - The purpose for which the information is being collected; and
 - The intended recipients of the information
- RHFL corporate or any person on its behalf holding sensitive personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.
- The information collected shall be used for the purpose for which it has been collected
- RHFL corporate or any person on its behalf shall permit the users to review the information they had provided and modify the same, wherever necessary.
- **Storage Transfer & Destruction of PII**
 - SPI will be accorded the same level of security as confidential information irrespective of the classification of such information. Please refer to Lifecycle Processes for Confidential Information for storage, transfer and destruction of SPI.
 - OPI will be accorded the same level of security as Restricted Information irrespective of the classification of such information. Please refer to Lifecycle Processes for Restricted Information for storage, transfer and destruction of OPI.

2.2 Asset Management


2.2.1 Purpose

To define practices for identification and cataloguing of Information Systems involved in usage, maintenance and disposal of information assets in order to protect information used by RHFL and achieve efficient and effective service delivery.

2.2.2 Scope

This policy applies to all information systems being used by RHFL or involved in creation, storage, transmission or destruction of RHFL's information, which includes but is not limited to the following:

- Software assets
- Physical assets
- People Services such as computing and communication services, air condition, power and document storage

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- Information – Digital asset & non-digital assets

Any individual handling RHFL's information assets in any form shall comply with this policy.

2.2.3 Policy

RHFL's information assets including hardware, software and physical assets used in the Company's physical environment and virtual premises such as hosting sites, service provider premises etc shall be managed in accordance with the information asset protection objectives established in this policy throughout the lifecycle of the asset i.e. from acquisition to its disposal.

Any breach of this policy shall be considered as an incident and shall be treated as per the incident management policy.

2.2.3.1 Information Asset Profiling

Information assets shall be classified using either quantitative or qualitative methodology chosen by the management, considering the below mentioned aspects:


- Data Information systems/equipment containing the data including paper format on which data might be stored in printed form.
- Data will be classified as per data classification policy.
- Other information assets will be classified to reflect business needs, legal-regulatory-certificatory requirements and confidentiality-integrity-availability concerns, based on the following criteria:
 - classifications of data contained in the asset
 - criticality of the asset to business operations
 - value of the asset exclusive of the value of data contained
 - form of data (hard copy/electronic) contained
 - usage of the asset (asset used to store, process, transmit data)
 - volume of data contained / transmitted through the asset

2.2.3.2 Lifecycle Processes

- Asset Acquisition Purchase

All assets shall follow a formal acquisition / purchase procedure. Assets shall be procured only after appropriate approvals are obtained from authorized personnel. All assets that have been procured shall be classified as per the asset profiling guidelines mentioned in this policy.

- Asset Tracking
 - Asset Labeling

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	


Every asset shall be marked for identification and inventory control. An appropriate set of procedures for asset labeling and handling shall be developed, and implemented in accordance with the classification scheme(s). This shall include:

- i. responsibility of the asset owner to assure/confirm classification and labeling, and subsequent handling consistent with that label;
- ii. classifications that cover all information processing facilities and information in all forms and media;
- iii. procedures for establishing ownership and chain of custody; and
- iv. Procedures for logging and reporting security incidents associated with the asset.

Determination of the frequency for periodic review to ensure that classifications appropriately reflect business needs legal-regulatory-certificatory requirements and balance confidentiality-integrity-availability concerns against other organizational goals.

○ **Asset Inventory and Documentation**

- i. A comprehensive inventory of all information assets shall be maintained.
- ii. Each asset shall be clearly identified individually and (if appropriate) collectively in combination with other assets to form an identifiable information asset.
- iii. The asset inventory shall include all information necessary in order to recover from a disaster.
- iv. The information asset inventory shall contain the following information as a minimum:
 - Identification
 - Description
 - Location
 - Owner
 - Custodian
 - Business value of the asset
 - Asset classification
 - Validity of the classification
 - Asset Support information
 - Hardware assets – Annual Maintenance Contract details
 - Software assets – Software License details
 - Physical Assets (documents) – Archival /storage arrangement

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- v. For every asset RHFL shall define service components or other items (Configuration Items) which are required to deliver or support one or more IT services.
 - vi. Configuration Items (CI) shall be grouped, classified and identified in a way such that they are manageable and traceable throughout the service life cycle.
 - vii. Methods shall be included to track CIs from ordering to depreciation. Change of data shall be controlled to ensure that it can only be altered by authorized individual.
 - viii. Status maintenance of CIs shall be consistently recorded and kept updated.
 - ix. RHFL's Configuration Items shall be listed in a configuration management database which shall contain all relevant details of each Configuration Items and details of the important relationships between Configuration Items
- **Authorization Inventory**
 - i. The asset inventory shall contain details of authorization mechanism for all information assets
 - ii. For RHFL owned assets, the authorization record shall consist of the owner and the features of the asset used to authorize the asset to the RHFL network such as the network interface media access control (MAC) address or the IMEI number.
 - iii. For non RHFL owned assets, the authorization record shall consist of parameters used for two factor authentication such as username and password, token ID or biometric record.
 - **Asset Use**
 - i. All RHFL assets shall be used as per the 'Acceptable Usage' of assets covered in Section 1.6 of General Policy.
 - ii. RHFL assets shall be used by authorized personnel for valid business purposes only and shall be stored in a physically secure manner at all times including when not in use.
 - iii. Assets shall be allocated to users based on job functions / business requirements. A record of such allocations shall be maintained by the IT / Admin teams.
 - iv. Assets shall be transferred among RHFL users however a formal procedure for the same shall be followed. A register of such transfers shall be maintained and updated by the IT / Admin teams.
 - v. Each user of end user assets and owners of enterprise assets shall be responsible for the assets owned / used by them and any activity done using these assets.
 - vi. To minimize the risk of theft, destruction and/or misuse all asset owners / users / custodians shall exercise good judgement and safeguard the assets that are being used by them / are in their custody and the information contained therein.
 - vii. Assets shall not be taken out of RHFL premises without appropriate authorizations. In scenarios where the asset may need to be taken out of RHFL premises for repairs

/ replacement appropriate authorizations shall be taken after ensuring that the data contained in the assets has been securely erased.

- viii. Employees who are possessing company provided mobile devices such as laptops, tablets, smart phones will have authorization to carry asset outside office premises.
 - ix. IT assets shall be hardened as per the hardening guidelines laid down in the 'Information Systems Acquisition and Development' section of this policy – 2.5'
 - x. All assets requiring periodic maintenance shall be covered under appropriate Annual Maintenance Contracts (AMCs) which shall be renewed and kept current at all times.
- o Asset Disposal
 - i. Asset shall be disposed of if:
 - The asset has reached end of life
 - The asset does not suit the environment
 - ii. Critical infrastructure elements which need to be disposed off shall be approved with valid justification by the CTO and CFO.
 - iii. Finance department shall also be informed as and when an asset is disposed off.
 - iv. Any information that resides in the asset shall be removed from the equipment before disposal using secure erase / disposal techniques that have been approved by the Management.
 - v. A register for all disposed / scrapped assets shall be maintained.

2.2.3.3 Loss / Theft of asset

- In case of loss / theft of personal device with access to RHFL Information assets, the employee shall report the same immediately.
- The IT function shall be responsible to immediately revoke all access to RHFL's Information Assets through the device, and shall attempt to remotely wipe off RHFL data from the device.
- In case the device loss / theft is reported after more than 4 hours, or if the remote wipe is unsuccessful, the same shall be recorded as an incident and incident management procedures as described in this policy shall be followed.

2.3 Access Control

2.3.1 Purpose

- To provide a set of practices for access to RHFL's information and information systems (Operating Systems, Applications, Databases, Network Equipment and others).
- Access controls pertaining to RHFL's information and information systems shall be based on principles of 'User Authorization' and 'Accountability' and support the security concepts of 'least privilege access' 'need-to-know', 'segregation of duties' and 'individual accountability'.

2.3.2 Scope

- This policy shall apply to all environments requiring logical access to information assets such as systems where information is stored or processed, communication and network connections through which information is transmitted or applications through which information is accessed.
- Communications and network connections include, but are not limited to network devices such as routers and firewalls; systems shall include but are not limited to servers and mainframes, storage tapes or drives, databases and applications.
- This policy applies to all users such as employees, contractors, service providers / visitors accessing RHFL's information assets.

2.3.3 Policy


- All user accesses to RHFL information assets shall be specifically and individually authorized based on business need. Security controls shall ensure that only authorized individuals can access RHFL information assets.
- Procedures shall be administered to ensure that appropriate level of access control is applied to protect the information in each system from unauthorized access, modification, disclosure or destruction to ensure that the information remains accurate and confidential, and is available when required.
- Any breach of this policy shall be considered as an incident and shall be treated as per the incident management policy.

2.3.3.1 User Identification and Accounts

- A User-ID or account shall be assigned to each individual to authorize a defined level of access to information assets, and shall be protected by authenticating the user to the User-ID upon requesting access.
- Each User-ID or account on RHFL information systems shall uniquely identify only one user or process. Every individual user shall be accountable for all actions associated with his /her User-ID. User-IDs shall not be utilized by anyone other than the individuals to whom they have been issued. Users shall not allow others to perform any activity with their User-IDs. Similarly users shall be forbidden from performing any activity with User-IDs belonging to other users.
- Where it is not possible to implement individual User-IDs and passwords within the system due to technology limitations or process design, alternative solutions for restricting and auditing access privileges shall be evaluated for feasibility and shall be implemented.

2.3.3.2 Group / Generic User IDs

- The use of generic and group User-IDs shall be avoided wherever possible. Wherever there is no alternative available / it is absolutely essential a group account shall be used; however it shall follow the Exception grant and risk assessment methodology requiring the prior authorization of the appropriate authorities and clear accountability to one individual (Group ID owner) shall be established. The use of Group-ID shall be short term in nature having an expiration date.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- Generic User-IDs shall not be created unless necessitated by technology limitations or under business exigencies. An owner shall be identified for every generic User-ID created and the owner shall be held accountable for all actions associated with the generic User-ID. Where it is required for a generic User-ID to be shared between multiple individuals, alternative solutions for assigning and ascertaining accountability at all times shall be evaluated for feasibility and shall be implemented.

2.3.3.3 User-ID Creation and Maintenance

- User-IDs shall be non-transferrable and individuals shall not have multiple accounts within the same computing environment.
- Access to RHFL’s environment such as the network shall be granted only upon intimation received from HR. All users shall be granted access to the information systems and services through a formal user registration process that shall include the approval of access rights from authorized personnel before granting access.
- All users shall follow a formal de-registration process for revocation of access to all information systems and services which shall include automated or timely intimation and revocation of access rights. Intimation for revocation of access rights shall come from HR. A confirmation of the access revocation shall be sent to HR as a part of the exit clearance process.
- Levels of access granted to all Users shall enforce segregation of duties, and adhere to the “need to know” principle. Where segregation of duties cannot be enforced by logical access controls, other non-IT-related controls shall be implemented.
- An initial password shall be provided to the users securely during the user creation process and the system shall be configured to force the users to change the initial password immediately after the first logon.
- Appropriate procedures shall be put in place for storing and management of administrative passwords for critical information systems. All user passwords shall be encrypted while in transmission and storage.
- The password requirements for all user accounts shall follow the password guidelines as defined in the Acceptable Usage - Password Standard. Any exceptions to the password standard shall follow the Exception grant and risk assessment methodology requiring the prior authorization of the appropriate authorities and counter measures shall be implemented to mitigate the resulting risk.
- The respective Department Heads for all individual users or user groups shall review the access rights or privileges assigned to the corresponding system periodically. Any exceptions noted shall be addressed at the earliest.
- In case of transfer of an employee from one function to another, access rights of the user shall be revoked for previous functional role and access need to be provided for new functional role.

2.3.3.4 User Authorization

- Users shall be authorized on RHFL’s information systems at the following levels:

- Physical access
- Network
- Infrastructure
- Endpoints
- Applications
- Cloud (where applicable)
- Limited access in line with access policies set by owners of business applications and systems
- User authorization mechanisms at each level shall be independent of authorization at a previous or subsequent level – for example, applications shall perform assessment of user authorization request independent of the operating system authorization process.
- Management and employees shall be responsible for controlling access to all facilities and ensuring that people entering or accessing those facilities are properly identified and authorized.
- All network and network services in RHFL shall be identified and documented. User shall be authorized at the network perimeter based on the profile of the network resource being requested to be accessed. Connection capability of the users shall be restricted through appropriate perimeter security devices such as firewalls, routers and switches.
- Access to all endpoints and applications shall be permitted only after authorization of the user credentials by the host operating system or the application itself.
- If the authorization request comes from a RHFL owned asset(device/network), single factor authentication will suffice. In case the authorization request comes from a non-RHFL asset (device/network) two-factor authentication will be mandatory.
- Applications hosted on the Cloud shall accept a user authorization record validated by a RHFL owned authorization service or require two factor authorization as stated in (6) above.
- Details of Business owner, approvers and their delegated authority shall be maintained and be re-certified and updated periodically. The authorization process shall include process for granting emergency access.

2.3.3.5 Privileged User Accounts

- Privileged user accounts are accounts with administrative access to applications, operating systems, network devices, databases components and other information systems enabling a user to modify system configurations including metadata, user records and other functions and override security and controls within the system to which administrative access applies. Privileged user account include (but not limited to), system default administration account, 'Administrator' or 'root' or equivalent operating system accounts or any User-IDs capable of creating, modifying or deleting other User-IDs or their privileges or access logs.

- Privileges associated with each type of information system such as Operating System, Business Applications, Databases, and Network Elements shall be identified and documented.
- Privileged user accounts shall be limited to individuals with specific business justification for this level of access. Such access shall only be granted upon authorization from appropriate personnel.
- Individuals granted this level of access shall have appropriate skill levels to perform security or administration duties for the system to which privileged access is granted.
- Use of the Privileged User ID shall be minimized to the extent possible. Activity from all logons with Privileged User ID shall be securely logged. Refer to 2.14 Monitoring, Logging and Assessment for further details on logging and monitoring of privileged User-IDs.
- Where feasible separate mechanisms shall be provided for logging-on to systems for privileged activities and routine activities. Where such mechanisms are available individuals with privilege user IDs shall logout out of privilege environment for performing routine day to day task which do not require such privileged access.

2.4 Human Resource Security


2.4.1 Purpose

To define RHFL's desired practices concerning human resource security to ensure that:

- The Human Resources function meets its requirements within the context of the corporate framework for the security of its information and equipment.
- Employees, contractors and third party users are aware of information security threats and concerns, understand their responsibilities and liabilities with regard to information security, and are equipped to support organizational security policy in the course of their normal work.
- Employees, contractors and third party user's entry, exit or change employment in an orderly manner.

2.4.2 Scope

- Human resources are an integral element of RHFL's security framework. The security of information resources requires the integration of knowledgeable and aware personnel, with appropriate technology enabled controls. Weak human resource security processes can result in security breaches, financial frauds, company reputation and regulatory non compliance in not meeting customer confidentiality.
- This policy shall apply to all employees, contractors and third party users using RHFL's Information Technology resources.
- Human resource (HR) security is a part of personnel management and applies to pre-employment, duration of employment and termination of employment.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

2.4.3 Policy

RHFL shall ensure that all users joining, moving within or leaving the RHFL network (employees, contractors and third party service providers), shall be aware of their roles and responsibilities with regard to information security. The HR practices of RHFL shall support its information security objectives at all times i.e. prior to employment, at the time of on-boarding, during the employment tenure and at the time of exit.


Any breach of this policy shall be considered as an incident and shall be treated as per the incident management policy.

2.4.3.1 Prior to employment

- All job roles and responsibilities shall be documented and shall include general as well as specific responsibilities for implementing or maintaining information security. All employees, contractors and third party service providers of RHFL shall understand their job roles and responsibilities.
- Background checks shall be performed on all personnel (including temporary and contract personnel) performing sensitive or critical job roles before they are selected for the position or transferred to the position. Further, personnel who are third party service providers shall have undergone a background check by their respective organizations and the assurance of the same shall be provided to RHFL. Information provided by the personnel, at the time of recruiting shall be subjected to verification procedures.

2.4.3.2 On-Boarding and During Employment

- All employees, contractors and third party users of RHFL's information assets shall sign their employment contract which shall include confidentiality agreements / non disclosure agreements (NDA) and shall be an indication of their acceptance to the terms and conditions of the contract which shall include protection of RHFL's confidential and sensitive data. These terms and conditions shall state the organization's as well as the employee's responsibilities towards information security.
- In some cases, an authorized representative shall sign an agreement on behalf of all contractors and third party users which shall appropriately address security considerations. If the information security provisions laid out in the agreement differ from the standard employee / contractor/ third party contracts, the same shall need to be taken through the Exception grant and risk assessment methodology.
- Processes and procedures shall be defined for reporting the violations of confidentiality agreements.
- All supervisory roles shall be responsible for the performance and conduct of the staff personnel reporting to them including the information security requirements laid down as a part of the employment contracts and the organization's policies. Managers or Supervisors shall be required to monitor the performance and conduct of each of their staff, as well as to assess their impact on the security of the information assets to which the staff has access.
- The punitive actions to be taken for violation of the information security requirements in the employment contract or the Information and Cyber Security Policy shall be as per the

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

‘punitive actions’ laid down as a part of the compliance section of the general Information and Cyber Security Policy.

- Information Security Training and Awareness Programs shall be provided to all the employees, contractors and relevant third party users of RHFL systems in order to create consciousness about the information security policies and processes.
- The information security function shall develop an Information Security Training and Awareness Programs which shall define, in addition to the content of the program, a timeline and periodicity for attendance to the program.
- Mechanisms shall be established to track the attendance of each staff for the training and awareness program. Any employee who fails to attend the training and awareness session as per defined periodicity shall be given a stipulated time to attend the same, failing which it will be considered non-compliance to this policy.

2.4.3.3 Exit Procedures

- RHFL shall ensure that termination of employees, contractors and third party users is performed in an orderly manner, and responsibilities are defined within RHFL to ensure the same.
- The assets of RHFL available with terminated individuals shall be taken back and all their access rights (physical and logical) shall be removed immediately.
- RHFL shall take into consideration the changes of responsibility or transfer of employees, contractors and third party users and assess the appropriateness of their access when such occasions arise.
- All employees, contractors and third party users shall return all of the organization’s assets in their possession, upon termination of their employment, contract or agreement.
- Mechanisms shall be put in place to ensure that access granted to any employee or contractor is revoked prior to the termination of their employment / contract period with RHFL. Controls shall be put in place to ensure that any failures to remove access for terminated employees or contractors is detected in a timely manner and acted upon immediately.
- Any IS violations during the tenure of the employee shall be reviewed before the final sign off.

2.5 Information Systems acquisition and development

2.5.1 Purpose

To define the desired practices for acquiring, designing, developing, testing and implementing information systems.

2.5.2 Scope

This policy shall apply to all information systems where RHFL’s information assets are stored or processed and all communication and network connections through which RHFL information assets are transmitted.

All Business Units or Departments using information technology shall comply with this Information and Cyber Security Policy.

This shall apply to developing new software, customizing software and developing software that can be accessed or presented on a website.

2.5.3 Policy

RHFL Information systems shall provide for maintenance of confidentiality, integrity and availability, of data contained within them, by design. This shall be achieved by processes, throughout the System Development Life Cycle beginning at acquisition through development and maintenance.

Any breach of this policy shall be considered as an incident and shall be treated as per the incident management policy.


2.5.3.1 Technology Standards

- **Infrastructure Standards**

- Security requirement analysis and specifications
 - i. Security requirements in an information system shall be identified and documented during the requirements gathering and analysis phase of acquisition, development or change of information systems. They shall be justified and agreed with business process owners.
 - ii. Systems security requirements shall reflect the business value of the information assets involved and the potential damage that may be caused due to absence of sufficient security.
 - iii. Minimum Baseline Security Standards (MBSS) shall be developed and maintained and all information systems shall be configured as per such standards.
 - iv. The MBSS shall include protection of data contained in the information system as well as system software used for operation of the information system itself.
 - v. All information systems (server, routers, and firewalls) shall undergo hardening as per the MBSS before being commissioned for usage in the production environment.
 - vi. The clocks of all relevant Information Systems within RHFL's security domain shall be synchronized with an agreed accurate time source.

- **Application security standards**

- Security requirement analysis and specifications
 - i. Security requirements in an information system must be identified and documented during the requirements gathering and analysis phase of acquisition, development or change of information systems. They must be justified and agreed with business process owners.
 - ii. Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- iii. Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.
 - iv. Systems security requirements must reflect the business value of the information assets involved and the potential damage that may be caused due to absence of sufficient security.
 - v. Applications shall be assessed for their security posture through security reviews before being commissioned for usage in the production environment.
 - vi. Application security reviews shall be conducted based on application security checklist and guidelines defined by the information security team which shall cover the aspects to be addressed in such reviews and provide guidance on requirements for conducting such reviews by external agencies.
- Correct Processing in Applications
 - i. Data input to applications shall be validated to ensure that this data is correct and appropriate.
 - ii. Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.
 - iii. Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.
 - iv. Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances
- **Availability Standards**
 - Information systems classified as critical for business operations shall be designed to support high availability operations by design of the system or the deployment of the same.
 - For all information systems requiring high availability, management shall carry out the following functions:
 - i. When an asset is procured, it shall be ensured that the asset configuration provides for fault tolerance.
 - ii. After procurement, system shall be configured at an availability mode depending on the level of criticality
 - iii. Develop a plan for availability monitoring, reporting and management.
 - iv. Optimize availability through monitoring and reporting of equipment performance.
- **Application Development**
 - A formal software development security framework shall be developed by the IT team..

- The software development security framework shall define a software risk assessment process to ensure that software security requirements are assessed considering associated business and technology risks.
- Modifications to software packages shall be discouraged. Vendor-supplied software packages shall be used with minimum modification unless they impact security posture of the software package vis-à-vis the Information and Cyber Security Policy.
- All modifications (including configuration changes, changes to reports, etc.) to software packages shall be made in accordance with formal Program Change Control Procedures.
- If the software is developed by a third – party the following shall be done –
 - i. RHFL shall ensure that software development processes followed by the third-party are in compliance to RHFL’s Information Systems Acquisition, Development policy.
 - ii. RHFL shall have appropriate licensing agreements and contractual requirements for quality and functionality of the application exist.
 - iii. Appropriate documentation in form of product manuals or data sheets shall be obtained from the third party to ensure that the security requirements of the Information and Cyber Security Policy are adhered to.
 - iv. Appropriate testing shall be carried out prior to the software being put in commissioned for usage in the production environment, to ensure that the requested functionality including security requirements are met by the software.
 - v. A formal methodology shall be defined and documented including security requirements for application development and maintenance process when done in-house.
 - vi. Test data shall be selected carefully, protected and controlled.


2.5.3.2 Risk Assessment of new technology

- **Scenarios**

- Technology Risk assessment shall be carried out for the following scenarios:
 - i. Introduction of new process or technology
 - ii. Changes to existing process or technology
- Technology risk assessment shall be performed by the respective IT or business team responsible for introducing the new process / technology or changes to them.
- Technology Risk assessment shall be carried out based on technology risk assessment templates and/or checklists defined by the IS team.

- **Technology risk assessment Process**

- Technology risk assessment shall be performed as per guidelines provided in ‘Information and Cyber Security Policy - General Policy 1.7 - Risk Management’

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- **Architecture and Interdependencies**

- Technical and functional architecture for any new Information Systems developed / produced by RHFL shall be reviewed and approved by the IS team from an information security perspective
- Interdependencies of the new information system being developed / produced shall be assessed with the overall RHFL environment from an information security perspective.

2.6 Information System Maintenance

2.6.1 Purpose

To define desired practices for maintenance of information systems with respect to protecting confidentiality, privacy and availability. Security has to be considered during operation of an information system including maintenance and retirement in order to:

- Ensure conformance with all appropriate security requirements
- Protect information assets contained in the information system
- Protect the system against new emerging risks
- Prevent the introduction of new risks when the system is modified
- Ensure proper removal of data when the system is retired.

This policy shall provide guidance to ensure that information security is considered during the maintenance of an information system's life cycle.

This policy defines RHFL's desired practices concerning Information Systems Maintenance.

2.6.2 Scope

This policy applies to all information systems where RHFL information assets are stored or processed, and all communication and network connections through which RHFL information assets are transmitted.


Technology systems, communications and network connections shall include but are not limited to network devices such as routers and firewalls, servers and mainframes, and systems, databases and applications.

All Business Units or Departments using information systems shall comply with this policy.

2.6.3 Policy

Appropriate maintenance shall be carried out to protect the confidentiality and integrity of information contained within and maintain availability of information systems.

Any breach of this policy shall be considered as an incident and shall be treated as per the incident management policy.


Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

2.6.3.1 Backup and Restoration

- The frequency of backup, frequency of restoration testing and requirements for storage of the backup shall be defined based on the classification of the data being backed up, in a backup and restoration checklist and guidelines defined by the Information Security team. Data restoration testing must be performed at a minimum of six months or more frequently, as required by the business.
- All applications and operating systems software, data (including databases), application and operating systems configuration information, hardware configuration information (where applicable) and log files that require to be backed up shall be identified and documented along with the medium and storage of the backup, location of the offsite media (if required) for the required system.
- All backup media shall be encrypted.
- A log of backed data restored from backup media shall be maintained.
- The number of backup sets to be maintained shall be decided based on the criticality of the information residing in the information systems.
- In addition to the scheduled backups, backups shall be taken in case of:
 - Configuration changes in any of the systems
 - Upgrade of an operational system.
 - All movement of tapes between offsite and onsite locations shall be tracked and recorded.
- To verify the readability of the backup media, mock restoration tests shall be carried out as defined in the backup and restoration checklist and guidelines, on the test systems periodically. The process shall be documented detailing the test plan, the activities carried out and the test results. Exception identified during the testing process shall be documented and reported.

2.6.3.2 Patch Management

- The team responsible for maintenance and monitoring of Information systems shall maintain an inventory of software components comprising the IT environment. Refer to Asset management policy on asset inventory.
- The team responsible for maintenance and monitoring of Information systems shall monitor announcements from providers of software (including application and system software such as operating systems and databases) for software ‘patches’ made available to remove security vulnerabilities.
- Each patch identified shall be taken through the following process.
 - The patch shall be evaluated for their relevance to RHFL, and determine whether it represents a normal or emergency change.
 - All patches shall be tested in the RHFL operated test environment for feasibility of their application in RHFL production environment.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- Business critical applications shall be reviewed and tested prior to installation of OS or database patches, in a test environment, in order to ensure that there is no adverse impact the application due to the changes in the operating system.
- Application of patches or updates for end-computing devices shall be performed such that the patches are effectively deployed on them, within reasonable time of the device gaining access to the RHFL network or enterprise information assets.


2.6.3.3 Job Scheduling

- A comprehensive inventory of scheduled jobs including daily, weekly, monthly, quarterly, and yearly batch runs or backup scheduled to be run on the production environment shall be maintained, including the interdependencies between jobs.
- All jobs that are run in the production environment shall be approved by the information system owners.
- All scheduled jobs shall be monitored for their performance, success/ failure, and the results shall be documented.
- The results of a scheduled job shall be reviewed within reasonable time and action shall be taken based for any non-standard behavior including failure of the scheduled job or it part thereof.
- Schedules shall be subject to change either through planned or emergency requests.
- The team responsible for maintenance and monitoring of information systems shall be responsible for scheduling and monitoring jobs with respect to the schedule.
- Any non-standard behavior including failures shall be raised as incidents and tracked for closure as per the incident management policy.
- All scheduled jobs shall be designed to delete any temporary files generated during the performance of the job, and not required after completion of the same.
- Controls shall be put in place to ensure that dependencies between various jobs are considered and failures impacting the dependencies are highlighted as alerts which can be monitored.

2.6.3.4 Capacity and Performance Management

Controls shall be put in place for monitoring the utilization and performance of information systems to ensure that availability requirements are met at all times.

- The results and logs of the monitoring activity shall be analyzed for occurrence of security incidents and incidents shall be tracked for closure as per the incident management policy.
- The results and logs of the monitoring activity shall also be used to identify trends which might require changes to the IT environment or augmentation of IT resources. The results of the analysis shall be used to develop a Capacity Management plan intended to help RHFL meet or exceed the performance targets.
- Thresholds shall be documented and monitored.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

2.6.3.5 Malicious Software Management

- All servers, desktops, workstations, hand-held devices, gateways and any other access points to RHFL’s network shall be protected against malicious activities (this shall include viruses, trojans, malware, adware, spyware and the like).
- Anti-virus application and processes shall be put in place to facilitate early detection, efficient containment and eradication of malicious code. Adequate user awareness measures shall be implemented for the same.
- Controls shall be considered to prevent unauthorized software execution.
 - Protection software such as anti-virus anti-malware, anti-spyware, and anti-adware needs to be installed on information systems controlled / used by RHFL.
 - The software shall be capable of being updated on a periodic basis from an authentic source of malicious software information.
- The software must provide real time protection. Malicious activity detected by the software shall be reported to an enterprise system which shall be monitored and unresolved malicious activity shall be raised as incidents and tracked for closure as per the incident management policy.

2.6.3.6 Vulnerability Management

- In addition to software based automated protection, the IS Operations team shall be responsible for keeping track of new vulnerabilities that could lead to a worm or virus attack by subscribing to security mailing lists of OS and application vendors, tracking virus alerts from anti-virus vendors and keeping track of advisories from independent security organizations like CERT.
- Upon identification of a new vulnerability relevant to RHFL, the IS Operations team shall identify the steps to be taken to ensure that the associated risks are mitigated.


2.6.3.7 IT Service Management

- RHFL shall have a defined and documented service catalogue for its IT services containing information about the currently available IT services at RHFL to provide a single source of consistent information of RHFL’s agreed IT services to all authorized users..
- Service levels shall be defined for each information system based on the business requirements.
- Mechanism shall be established to monitor service levels and analyze breaches of service levels. Any service level breaches impacting information security shall be raised as incidents and tracked for closure as per the incident management policy.

2.7 Change Control

2.7.1 Purpose

To define consistent and systematic practices for efficient and prompt handling of all changes to RHFL’s information resources in order to minimize the impact of the changes on information assets.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

2.7.2 Scope

Any change to RHFL's information all assets either in electronic form or electronic record or hard copy that may affect the resources upon which the organization relies to conduct normal business is within the scope of this policy. The following non-exhaustive list depicts common type of changes:

- Software upgrades, updates or additions
- IT Infrastructure changes
- Preventative maintenance
- Security patches
- System architecture and configuration changes
- Hardware upgrades
- Product management

2.7.3 Policy

All changes to RHFL's information resources shall be performed in a controlled manner to ensure that the risks associated with such changes are managed to an acceptable level. Formal procedures for change management shall be documented and all changes to RHFL's information assets shall follow the standard change management procedure.

Appropriate procedures shall be put in place for all changes requiring emergency actions and response process, which bypass the Policies and Procedures outlined.

Any breach of this policy shall be considered as an incident and shall be treated as per the incident management policy.

2.7.3.1 Change Governance


Change governance will be followed as per IT governance framework.

2.7.3.2 Change Classification


- All changes shall be classified based on the following factors:
 - Data impacted by the change
 - Impact of the change on RHFL's IT environment.
- All changes shall follow the change lifecycle mentioned below and require appropriate approvals based on the classification of the change. Major changes and "Identified CR types" shall be put through a Technology Risk Assessment (TRA) which shall be performed by the IT Team based on TRA standards defined by the Information Security team. Results of TRA shall be reviewed by the Information Security team on periodic basis.

2.7.4 Change Lifecycle

- Separate environments shall be created and maintained for development and testing of changes to information systems

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- The test and development environments shall, at a minimum, be physically or logically segregated from production systems while ensuring that no user has access to both environments simultaneously.
- Production data shall preferably not be transferred to the test / development environments. In situations where the production data needs to be transferred to the test / development environments the same level of protection as the production environment shall be applied to these environments; else production data shall not be moved to these environments.
- All changes to RHFL's information assets shall adhere to the following change lifecycle:
 - Request for change – request for the change shall be formally raised and recorded. This shall be followed by a formal business requirement definition, impact and feasibility analysis as applicable.
 - Impact analysis shall need to be performed by the change requestor and include assessment of potential Financial, Operational, regulatory, technology and other impacts.
 - Change approval – all changes shall be duly approved by appropriate individuals as per the change authorization matrix defined by the IS team.
 - Prioritization of changes – changes shall be prioritized by the change implementation team(s) based on the criticality of the change and the impact of the change on the information asset.
 - Testing of changes – all changes shall be tested in the test environment. This shall include different levels of testing such as System Acceptance Testing (SAT), System Integration Testing (SIT), User Acceptance Testing (UAT) etc depending upon the type of change, as defined in the change management procedure by the IS team.
 - Migration- all changes shall be migrated to the production environment after appropriate approvals and by authorized individuals. Restrictions shall be maintained to ensure that access to the production and development / test environments is duly segregated
 - Documentation update – all relevant documentation shall be updated to reflect the impact of the change. All records of testing shall be formally documented and maintained.
- Emergency changes as defined in the change management procedure shall be exempted from following the change lifecycle mentioned above due to the urgent nature of the change.
- All emergency changes shall however be appropriately documented and post-facto approvals from relevant authorities shall be obtained.
- Details of Business owner, approvers and their delegated authority shall be maintained and be re-certified and updated periodically. The authorization process shall include process for granting emergency access

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

2.7.4.1 Release Management

- Releases to both packaged and bespoke applications within RHFL shall follow the formal release management process.
- The release management process of RHFL shall have the following considerations:
 - For releases issued by third parties, appropriate delay shall be allowed before a new release is implemented to allow for any initial problems with the release to be known and sorted out by the provider.
 - All release related communication shall be sent to the relevant stakeholders well in advance of the release.
 - Appropriate version control procedures shall be followed to ensure the release and its supporting documentation is version controlled.
 - A release document shall be prepared and provided along with every release which shall contain details about the release such as goals and objectives, process flows, release planning, release building, acceptance testing, release preparation, release deployment and roles and responsibilities.

2.8 Incident and Problem Management

2.8.1 Purpose

An Incident is defined as the occurrence of any exceptional situation that could compromise the Confidentiality, Integrity or Availability of Information assets of RHFL. Problem Management includes the activities required to diagnose the root cause of incidents and to determine the resolution to those problems.


This policy defines RHFL's desired practices concerning Incident and Problem Management.

2.8.2 Scope

This policy shall apply to all incidents resulting from violation of Information Security policies or processes / guidelines defined by the Information Security team based on the policy. These include but are not limited to:

- attempts (either failed or successful) to gain unauthorized access to a system or its data
- unwanted disruption or denial of service
- the unauthorized use of a system for the processing or storage of data
- changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent

All Business Units or Departments using information technology must comply with these Information Security Policies.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

2.8.3 Policy

RHFL shall implement procedures for detecting, reporting and responding to incidents in routine administration of information security and for analyzing and tracking their closure.


Any breach of this policy shall be considered as an incident and shall be treated as per the incident management policy.

2.8.3.1 Reporting IS Event and Weaknesses

- All users shall be expected to report incidents in a timely manner. Mechanisms shall be established for all users of information systems to report incidents.
- Mechanisms shall be established for monitoring of information systems to detect any malfunctions (any abnormality or deviation in functioning); all such malfunctions shall be recorded and analyzed, and those resulting in violations of RHFL's security policies and procedures shall be considered incidents.
- Incidents shall be reported through the established mechanisms only in reasonable time.
- All contractors and third parties shall also be made aware of the procedures for reporting different types of incidents (like security breach, threat, weakness, or malfunction) that might have an impact on the security of information assets.
- All reported incidents shall be logged, analyzed and classified according to predefined criteria.

2.8.3.2 Incident recording and classification

- All incidents reported shall be recorded along with details mandated by the IS team, which shall include (but not limited to):
 - Source of the incident – user reported or through monitoring mechanism
 - Impacted information asset(s)
 - Incident description (details such as malfunction report, alerts and internal communications)
 - Time and date of the incident occurred, detected and recorded
- All incidents shall be classified into High, Medium or Low severity, based on the following criteria as per guidelines defined by the IS team:
 - Impact on information assets (breach of confidentiality, integrity or availability)
 - Scope of the impact (users, departments, locations, information systems)
 - Classification of data impacted
- All incidents shall be categorized as IS incident, IT incident, Non IT Incidents.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

2.8.3.3 Escalations and Tracking

- Escalations and actions shall be as per the classification of Incidents. Appropriate contacts with relevant authorities shall be maintained to escalate to the respective authorities as required.
- All high and medium severity incidents shall be reported to the CISO. All low severity incidents shall be reported to the BISO.
- All High and Critical incidents to be reported to CERT-in(Indian Computer Emergency Response Team) & CERT-Fin (Computer Emergency Response Team for Financial Sector) along with CISO, CIO & CRO

2.8.3.4 Management of IS Incidents and Improvement

- Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.
- Mechanisms shall be established to analyze all incidents in reasonable time and contain the impact of the incidents to the least possible scope.
- Mechanisms shall be established to resolve all incidents within timelines defined by IS teams for the incident’s respective classification.
- Mechanisms shall be established to recover any loss or damage to information assets as a result of the incident.
- Mechanisms shall be put in place to learn from incidents and enable the types, impacts, and costs of incidents and malfunctions to be quantified and monitored.

2.8.3.5 Root Cause Analysis and Problem Management

- Incident records shall be analyzed on a periodic basis to identify problems to proactively identify trends or to diagnose the root cause and any contributing causes for incidents in order to take preventive measures reducing the chance of reoccurrence of incidents
- Problems identified shall be assigned to individuals for resolution for identification of solutions within timelines agreed based on criticality of source incidents for the problems.
- Upon determination of the resolution to identified problems, corrective steps shall be implemented through the appropriate control procedures, especially Change Management processes.

2.8.3.6 Knowledge Management

- Mechanisms shall be established to record the resolution and known causes of incidents and problems in a knowledge base.
- Incident management teams shall be provided access to the knowledge base to reduce the time to respond to incidents.

2.9 Network Security

2.9.1 Purpose

To define RHFL's desired security requirements for protection of the IT network used or controlled by RHFL.

2.9.2 Scope

- This policy shall apply to all communication and network connections through which RHFL information assets are transmitted.
- Communications and network connections include but are not limited to network devices such as routers and firewalls, servers and mainframes.
- All Business Units or Departments using information technology must comply with these Information Security Policies

2.9.3 Policy

- Networks (connectivity infrastructure and related devices) used for RHFL's communication or under RHFL's control shall be appropriately secured to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of RHFL information.
- RHFL network shall be used for valid business purposes only. This means that access privileges shall not be authorized for an individual unless a legitimate business justification exists. The facility to access RHFL network shall be provided to users only after formal approvals.
- Network resources belonging to or under control of third parties that has been entrusted to RHFL shall be protected in the same manner as RHFL network resources and in accordance with other agreement. Shall there be a conflict between this policy and an agreement signed with a third party, appropriate provisions need to be made in the agreement to mitigate the risks and the agreement shall prevail thereafter.
- Any breach of this policy shall be considered as an incident and shall be treated as per the incident management policy.

2.9.3.1 Network Connectivity

- **Modes of Connectivity**
 - The modes of connectivity to RHFL Internal Network from an external location shall be only through authorized MPLS Cloud, Point to Point or through the Virtual Private Network. An authorized user shall be able to connect to the network via either of the below mentioned mechanisms:
 - i. MPLS
 - ii. Broadband & VPN
 - iii. WiFi

iv. Wired Network

- Any network connection allowing access to RHFL’s information asset shall be protected using perimeter devices such as firewalls or routers or other equivalent infrastructure to ensure that computer connections and information flows do not breach the access control requirements of RHFL’s policy.

- **Types of Connectivity**

- Only trusted entities shall be allowed full access to the RHFL network.
- All entry points to the RHFL network shall be reviewed and approved.
- Access to the network shall be via a secure log-on procedure, designed to minimize the opportunity for unauthorized access.
- All policies within the Access Control Policy shall apply to network connectivity.
- All connections via corporate computer and communication system shall be protected by authenticating connected users, devices or services.
- Any connection to RHFL’s IT Assets classified as business transaction systems and high severity systems from outside RHFL owned or controlled network (ex. remote connections), shall require two factor authentication as defined in the access control policy and compliance check validates the device connecting.


2.9.3.2 *Perimeter Security*

- **Identification of perimeter devices**

- RHFL shall deploy perimeter security systems (Firewall, IDS, etc) and develop and implement procedures, to protect all information assets from unauthorized or illegal access at the network level.
- An inventory of all perimeter devices shall be maintained and procedures set up to update the same on a periodic basis and upon every change in the network configuration.

- **Baseline security standards**

- Minimum Baseline Security Standards (MBSS) shall be defined for all types of perimeter security devices for all variants (make / model / versions) of the devices.
- Any changes to the baseline security standards shall be subject to the Change management policy.
- Mechanisms shall be implemented to ensure that network security resources adhere to the baseline security standards and any deviations in actual configurations and baseline security standards are detected and addressed or approved as exception where required to be retained.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

2.9.3.3 Network Management

- All network equipments and communication lines shall be identified, documented and updated regularly.
- Network diagrams for local and wide area networks shall be maintained and updated regularly.
- Security systems operating within and across public and RHFL networks shall be protected against internal and external intruders. The systems shall be installed in a physically secured and access-restricted area.
- The use of personal communications equipment (modems, ISDN cards, datacards, 3G data SIM etc.) attached directly to personal computers with remote control software shall be prohibited.
- Access to all communication equipment shall be subject to the access control policy, including the avoidance of generic user accounts.


2.9.3.4 External Networks

- Network traffic directed towards public networks such as the Internet shall pass through gateway systems such as the Proxy server, in addition to appropriate perimeter security systems, for implementation of access controls and related security mechanisms as per the access control policies.
- Access to external network resources shall be based on business requirements which shall include adherence to access control procedures.
- Connecting RHFL mobile assets to unauthorized WiFi access points and Hot spots shall be prohibited.
- User awareness training shall include acceptable use and cautions, copyright issues and disciplinary action for violation of acceptable use policy and general Internet ethics.
- RHFL shall reserve the right to monitor user actions on public networks, when such networks are accessed through information systems owned or controlled by RHFL, in order to protect the confidentiality of RHFL's information assets.
- RHFL shall implement adequate controls or contractual provisions for adherence to the network policy by third parties involved in providing network related services or having access to (or part thereof) RHFL's network resources

2.10 Cryptographic Controls

2.10.1 Purpose

To define the desired practices for use of cryptographic controls for protection of confidentiality and integrity of RHFL's organizational assets.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

2.10.2 Scope

- Cryptography is the practice of techniques for secure communication in the presence of third parties and utilizes encryption as a mechanism to encode information in such a way that eavesdroppers cannot read it, but authorized parties can.
- This policy shall apply to all forms of cryptography applied either to encrypt information in transit or at rest.
- This policy shall apply to all information systems where RHFL's information assets are stored or processed, and all communication and network connections through which RHFL Information Assets are transmitted which utilize cryptography as a mechanism for security of the information asset.

2.10.3 Policy


- RHFL shall ensure that appropriate cryptographic controls are applied to data depending upon its classification as per encryption requirements defined in the data classification policy.
- Any breach of this policy shall be considered as an incident and shall be treated as per the incident management policy.

2.10.3.1 Use of Cryptographic Controls

- Risk assessment shall be carried out to identify the needs, methodology, business areas and usage of encryption or cryptography.
- Cryptographic controls shall be used for securing information that is confidential and restricted.
- The definition of Confidential and Restricted Information will be based upon the respective classification ascertained by the Information Owner as per the Data Classification Policy.
- Critical information that is not actively used, when stored or transported in computer-readable storage media (such as servers, magnetic tapes, floppy disks or CDs, hard disk of mobile assets such as laptops and memory chips of mobiles), shall be in encrypted form wherever feasible and applicable.
- Information used to verify the identification of remote terminals shall be appropriately protected. Static or reusable authentication information shall be encrypted during storage and while passing through the network using encryption software or hardware.

2.10.3.2 Key Management

- Type and strength of the encryption algorithm to be used in a given situation shall be based on the criticality of the business information handled.
- The length of the cryptographic keys shall comply with contractual requirements and regulations laid down by competent authorities.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	


- Where possible, encryption keys shall not be transmitted over the network. If the keys used to govern the encryption process are to be transmitted over the network then they shall be transmitted through secure communication channels.
- Key management life cycle shall be comprised of following stages. Each component represents a set of processes that shall be addressed both in documentation and in practice:
 - Generating - Key generation shall be conducted in a secure environment (hardened system), and shall include the need to conform to requirements for separation of duties. Key generation procedures, guidelines to be referred for further details.
 - Storing - The storing shall imply writing the key to external media (e.g., CD, DVD, USB drive) and storing it in a physical vault. Key storing procedures, guidelines to be referred for further details
 - Archiving - If Retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys shall only be used for decryption/verification purposes. Key archiving procedures, guidelines to be referred for further details.
 - Distributing - The new key shall be deployed and tested for a pre-determined period of time to ensure that operations with the new key are successful before risking a data outage. Key Distribution procedures, guidelines to be referred for further details.
 - Retrieving – All access, retrieval of keys must go through Key retrieval procedure and guidelines.
 - Monitoring – Monitoring for unauthorized administrative access to crypto systems shall take place to ensure that unapproved key management operations are not performed. All cryptographic keys shall be protected against modification and loss.
 - Retiring - The chosen strength of an encryption key shall primarily take into consideration the length of time for which the data may be valid.
 - Destruction - Key destruction shall follow secure deletion procedures so as to ensure that it is properly obliterated. Key destruction procedures, guidelines to be referred for further details.

2.11 Business Continuity Management

2.11.1 Purpose

RHFL's ability to continue operating as a viable business entity depends on having proper contingency plans and procedures in place. If a business disruption occurs, RHFL must be able to resume operations in a reasonable time frame without compromising security.

This policy defines RHFL's desired disaster recovery practice to ensure adequate mitigation of risks from interruption of Information Technology services.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

2.11.2 Scope

This policy shall apply to all office locations and systems through which RHFL’s information assets are stored or processed, and all communication and network connections through which RHFL information assets are transmitted.

Technology systems, communications and network connections include, but are not limited to, network devices such as routers and firewalls, servers and mainframes, all operating systems, databases and applications.

2.11.3 Policy

All RHFL information systems and assets shall be protected against potential failure or disruption of service through a formal business continuity plan and disaster recovery plans that:

- Restores assets in accordance with system or asset criticality to RHFL business processes.
- Maintains the required level of security over RHFL’s information assets in the event of a disruption.

Any breach of this policy shall be considered as an incident and shall be treated as per the incident management policy.


2.11.3.1 IT Availability Management

- **Capacity monitoring and planning**
 - RHFL shall continuously monitor the utilization and make projections for future requirements of information processing resources and plan accordingly to ensure that adequate information processing resources are available to meet the business requirements of RHFL.
- **System acceptance**
 - Acceptance criteria for new information systems, upgrades and new versions shall include their ability to be resistant to disruptions or faults through appropriate design and configuration and suitable tests to determine such capability shall be carried out prior to acceptance.
 - Where resistance to disruptions is not provided for through appropriate design and configuration, alternative mechanisms to provide for resistance to disruptions shall be evaluated for feasibility and implemented where feasible.

2.11.3.2 IT Continuity Management

- **Data Back-up**

All data shall be backed up on a regular basis as per the Backup and recovery policy and the backups must be available for timely restoration in the event of information loss or disruption to ensure continuity of RHFL’s operations. Refer to Information Systems maintenance policy for details on backup management and restoration. The DR environment shall be kept in sync with the production environment at all times. All changes being applied to the production environment shall be applied to the DR environment as well to ensure the environments are in sync.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- **IT Continuity planning**

An IT Continuity plan or disaster recovery plan shall be developed for each RHFL entity or system based on appropriate risk assessment and business requirements and shall be approved by the ISRMC.

2.11.3.3 BCM Framework

RHFL’s BCM framework shall consist of documented business continuity and disaster recovery plans. A single framework shall be maintained to ensure all plans, across businesses and processes are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance. The BCP/DR plans shall address at a minimum:

- i. Enterprise-wide business continuation
- ii. Continuation of critical applications
- iii. Data Center Disaster Recovery Plans
- iv. Network connection / link
- v. Roles and responsibilities of all individuals in the Business Continuity and Disaster Recovery Plans

- **Outsourced relationship management**


All information and applications outsourced to a third-party service provider shall include adequate plans for continuity of service developed and tested by the third-party service provider and approved by RHFL. A RHFL liaison with the third party service provider shall supervise execution of the disaster recovery activities in the event of a disruption of service to RHFL.

- **IS consideration in BCM**

- A managed process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization’s business continuity.
- A comprehensive Business Continuity Plan (BCP) shall be developed and implemented in order to maintain or restore business operations in the required time scales following interruption to, or failure of, critical business processes. The BCP shall include effective Disaster Recovery procedures for quickly recovering from an emergency with minimum impact to the company’s operations.
- Business Continuity Plan shall be developed based on critical business processes and the likely disruptive events along with their probability, impact and consequences for information security identified through Business Impact Analysis.

- **Testing of BCP**

- The business continuity and DR plans shall be tested regularly tested at least bi-annually or when significantly changed to identify incorrect assumptions, oversights, or changes in equipment or personnel.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- Test results shall be reported to the ISRMC and shall be used to revise the BCP / DRP

- **Review of BCP**

- BCP shall be reviewed as per periodicity defined in the BCP itself and after each test and updated to ensure that the BCP considers the effectiveness of the current nature of business processes, infrastructure, personnel, etc

2.12 Third party service providers

2.12.1 Purpose

To define desired practices concerning the selection, enrolment, and termination of third parties and operations handled by them.

2.12.2 Scope

- This policy is applicable to all third party service providers such as contractors, vendors and consultants who handle, store or transmit RHFL's information and information resources in any form.
- This policy also applies to all information systems information assets and all communication and network connections owned, operated or managed by third parties, through which RHFL information assets are transmitted, stored or processed.
- Technology systems, communications and network connections include, but are not limited to, network devices such as routers and firewalls, servers and mainframes, all operating systems, databases and applications.
- All Business Units or Departments utilizing the services of a third party for business operations shall comply with this policy.


2.12.3 Policy

All contracts with Third Party service providers shall require that the third-party service providers provide controls to comply with provisions of the Information and Cyber Security Policy for RHFL information assets accessible to them,

This shall be deemed to conclude that the third party shall provide security at a level at least as secure as RHFL would provide internally. In addition:

- If confidential information is involved, a nondisclosure agreement shall be signed.
- Assessment of the third-party service provider for compliance shall be included in the agreement. Exchanges of information assets between RHFL and any third party may not proceed unless and until a written agreement has been reviewed and signed.
- All third-party service providers and contractors shall be under signed contract with RHFL before access to RHFL information assets can be granted.

Any breach of this policy shall be considered as an incident and shall be treated as per the incident management policy.


Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

2.12.3.1 Vendor IS Classification

- All third party service providers shall be classified with respect to Information Security based on a third party service provider classification guidelines defined by the Information Security team. The third party service provider classification standard shall consider the following parameters:
 - Nature of the activity performed by the service provider
 - Classification of information assets accessed by the third party.
 - Access to non information assets including RHFL premises
 - Criticality of operations of the third party
 - Access to RHFL’s Intellectual property
 - Providing services having a regulatory significance
 - Exclusivity and availability of multiple service providers in that line of service or geography
- The third party service providers classification guidelines shall define the information security requirements, periodicity and mechanism of compliance assessment and contractual requirements (such as escrow or service level requirements), for each class of third party vendors.

2.12.3.2 IS provisions in contracts and SLAs

- All third party service providers shall be empanelled for the services of RHFL only after a contract is signed between RHFL and the service provider.
- The contracted terms and condition shall be drafted by the Legal department of RHFL for safeguarding the interest of RHFL in consultation with Compliance, Risk and IS departments.
- The contract shall define, in addition to the services to be performed by the service provider, information security requirements to be adhered to while performing the service depending upon the classification of third party service provider as defined in the third party service provider guidelines.
- The service level agreement shall be drafted by business department at time of empanelment of service provider and shall be monitored on a periodicity defined in the third party service provider guidelines.
- In order to be able to enforce performance, information security and other controls to address outsourcing risks, RHFL shall build the right to audit as part of contract with vendors.
- If the vendor is certified under the ISO27001 standard, and if the scope of services provided to RHFL is included under the scope / statement of applicability for the certification, the vendor may be accepted from the requirement for periodic audits by RHFL. However, in such a scenario, the vendor will be required to furnish the following:
 - A self certificate of compliance to all IS provisions in the contract

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	


- Copy of a valid ISO27001 certification demonstrating that the scope of services provided to RHFL is included under the scope / statement of applicability for the certification

2.12.3.3 Enrolment and change

- The business department proposing to outsource an activity shall perform appropriate due diligence on the shortlisted vendor to assess the capability to comply with information security obligations in the contractual agreement. The due diligence shall be performed based on the classification of the third party service provider guidelines through either the following means:
 - Self-appraisal by the vendor;
 - On-site visit by RHFL personnel
 - Information collected from other public sources.
- Due diligence process shall involve evaluation of all available information about the service provider such as:
 - Past experience and competence to implement and support the proposed activity over the contractual period;
 - Business reputation and culture, compliance, complaints and outstanding or potential litigation;
 - Security policy, procedures and internal control, audit coverage, reporting and monitoring environment, Business continuity management;
 - Third party demonstrable level of maturity in relation to information security and their degree of commitment to information security. This is via a self-assessment checklist covering their maturity in the area
 - External factors like political, economic, social and legal environment of jurisdiction in which the service provider operates and other events that may impact security posture of the service provider;
 - Procedures in place for ensuring due diligence of its employees by the service provider
- The due diligence shall be performed at the time of enrolment of a new service provider or in event of changes to the services being provided by an existing service provider.

2.12.3.4 Periodic assessment

- Every third party service provider shall be assessed on a periodic basis to ensure that they remain compliant with the requirements of the agreements and information security requirements of RHFL, as per the periodicity defined in the third party service provider guidelines.
- The periodic assessment shall cover (not limited to) the following:
 - Services mentioned as part contract are performed as per SLA;

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- Personnel employed by service providers:
 - i. are competent with knowledge of product and processes handled
 - ii. are not barred by regulator or other legal authorities;
- Adequate infrastructure to perform the services;
- Adequate documentation of customers, bank and service records;
- Potential conflict of interest
- IS provisions as defined in the contract
- Access management for third parties including granting access, review of user access rights shall be periodically assessed and changed as applicable.

2.12.3.5 Termination

- RHFL shall reserve the right to terminate the services of any third party service provider on non-performance or non-conformity to any of RHFL’s contractual requirements including information security requirements. The clauses for termination shall be clearly laid out in the contract with the service provider.
- Upon termination or expiry of the contract, through natural expiry of the period of the contract or due to invocation of termination clauses by either party, the following requirements shall be adhered to:
- The service provider shall be expected to return any assets that belong to RHFL which are in the possession of the service provider during its tenure of service.
- Access to RHFL’s Information assets and premises, provided to the third party service provider’s personnel or systems shall be revoked with immediate effect or on the date of contract expiry to ensure the service provider does not continue to access RHFL’s information systems / premises.

2.12.3.6 Data Sharing and retention

- Valid business purpose must be defined for the data that needs to be shared with the Third Party Service Provider.
- Any data generated by the third party in the course of its operations performed for RHFL shall belong to RHFL and shall follow RHFL’s policies.
- RHFL Data, when it is in control of the third party will have to be subjected to the same or more stringent controls based on the classification of the data as per the requirements laid down in the IS policy.
- RHFL shall have the right to delete company related information from the vendor assets used for the activity, and certify it as per the data retention policy.
- Upon the termination of the contract all data transferred by RHFL or generated by the third party for RHFL, shall be handed-over to RHFL.

- Data, when in transit shall be subjected to the same or more stringent controls, based on the classification of the data as per the requirements laid down in the IS policy.
- Data will not be shared by the third party with any other entity apart from RHFL without explicit approval from RHFL and without an explicit contract which mandates compliance with RHFL policies.
- In case of third party including Call Centre operations, the Operating system has to be hardened to prevent data leakages.

2.13 Physical and environmental security

2.13.1 Purpose

To define the desired practices concerning physical and environmental security at RHFL for ensuring a secure environment for its employees as well as its tangible and intangible assets.

The physical security policy of RHFL shall aim at ensuring a secure environment for its employees as well as its tangible and intangible assets.

2.13.2 Scope

Physical Security provides the fundamental layer of control on safety, security and maintenance of People and Assets (including premises and infrastructure). Physical threats are important business risk as continuity of business operations depends on safety of people and infrastructure (including operating premises and information systems).

This policy applies to all assets of RHFL i.e.

- People such as employees, contractors, service providers / visitors accessing the RHFL facilities.
- Infrastructure such as building premises, furniture and fixtures, office equipment, physical documents and other electro-mechanical installations

2.13.3 Policy

All assets of RHFL (People and Infrastructure) shall be protected from unauthorized or illegal access as well as business and environmental threats.

Any breach of this policy shall be considered as an incident and shall be treated as per the incident management policy.

2.13.3.1 Zoning and Perimeter Definition

Facilities of RHFL shall be categorized into different zones based on the activities performed in them or the installations found in them. Correspondingly each zone shall have different levels of security. The classification into zones is detailed in sub-sections below:

- **Zone 1 or Semi- Public Zone**

Zone 1 shall essentially be the area within building premises between the entry gate and the point of entry protected by an access control system. The same shall be accessed with

minimal restrictions. In general, the front hall, meeting rooms and reception which are open to the general public shall be considered semi-public zones.

- **Zone 2 or Controlled Zone**

Zone 2 shall be the primary work area which can be accessed only after a thorough verification of the identity of the individual. Zone 2 shall be open only to authorized individuals who have been duly identified and have a business purpose to enter this area.

- **Zone 3 or Secured Zone**

- Zone 3 shall be a demarcated zone containing confidential data, sensitive or valuable assets (non-electronic) which require enhanced protection. Access to Zone 3 shall be highly restricted and shall be granted only on an absolute need basis. The specific individuals having access to this Zone could be:

- i. A special team within RHFL
- ii. External service providers required to access the Secured Zone for business purposes

- Some of the areas within Zone 3 would include:

- i. Dealing Room/ Trading Floor
- ii. Operating areas where cash and valuables are kept
- iii. Compactor rooms

- **Zone 4 or Electronically Sensitive Zone**


- Zone 4 shall be a demarcated electronically sensitive zone containing electronic assets which may host RHFL's data. This may include sensitive assets or systems which require enhanced protection. Access to Zone 4 shall be highly restricted and shall be granted only on an absolute need basis. The specific individuals having access to this Zone could be:

- i. A special team within RHFL
- ii. External service providers required to access the Secured Zone for business purposes

- Areas within Zone 4 would include:

- i. Server rooms
- ii. Datacenters
- iii. Hub Rooms

- RHFL shall ensure that Zone 3 and Zone 4 spaces are away from the entry/exit points in the building. Their location must not be displayed explicitly.


Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- Each Secured Zone shall have a designated owner. The Secured Zone owner shall be responsible for
 - i. Identifying the persons (internal staff and outside contractor, suppliers and visitors) authorized to access the Secured Zone
 - ii. Validating the list of persons authorized to enter the Secured Zone on a periodic basis
 - iii. Revoking all unnecessary / unauthorized access rights to the Secured Zones
- If an employee is found breaching the policy laid down for Zone 3 and 4 by the security personnel, the incident shall be reported to the site in charge (admin personnel) and BISO for taking actions as mandated by the procedure followed at the particular site. In case there is no procedure defined, the BISO shall escalate the matter to the ISRMC and shall thereafter take appropriate action as deemed necessary and also establish a formal procedure if felt necessary.

2.13.3.2 Physical Access Standards for Zones

- **Zone 1**

- Building / Premises (referred to as 'Premises' henceforth) shall refer to areas under the direct management control of RHFL management as defined below:
 - i. In case the entire structure is owned or leased by RHFL management, premises starting from the entry / exit gates to the structure from the public access street level shall be referred to as Premises under management control of RHFL.
 - ii. In case where RHFL has leased parts / owns only part of a building, Premises under management control shall refer to the Floor / Wing or any specific work area physically segregated from the rest of the building for purpose of ownership. RHFL shall request the premises authority to comply with its policies to the extent possible to ensure safety of its own assets.
- Access to Premises shall be granted to all people requiring access to them for professional reasons such as carrying out duties of work (employees / contractors / service providers) or seeking services from any RHFL entity (clients).
- Entry to Premises shall not by default entitle access to work areas or restricted areas but shall only allow access to Zone 1 (areas accessible to general public for professional purposes). This shall include (not exhaustively) the following:
 - i. Lobby / Reception
 - ii. Meeting rooms in the entrance lobby
 - iii. Cafeteria if it is outside the perimeter requiring access badges for entry / exit
- Access to Zone 1 shall be protected from unauthorized access by safeguards such as security guards stationed at entry / exit gates of the Premises.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- Security guards shall be stationed at the main entrance to protect against unauthorized access to the location premises. The guard shall be on duty 24x7. An administration team member shall be appointed as 'in-charge' for each RHFL Premises and shall be responsible to implement the policy for the Premises. In case of premises not having dedicated person, the respective branch manager / Head of the Business, shall be responsible to implement the policy for the premises.
- Certain individuals notified by RHFL Management can also be restricted from accessing the Premises open to general public. Such a restriction shall need to be notified by the BISO and the in-charge of Premises for each building and shall need to be approved by ISRMC.

i. For Employees / and Long Term Contractors

All employees of RHFL and contract staff who are authorized to enter the premises shall be provided with access cards (badges) identifying them to the organization. Access to Premises shall be granted upon display of identification badges issued to the employee / long term contractors. The access cards possessed by the employees / contractors shall grant them access to the premises by default.

ii. For Service Providers/ Visitors

Service providers and Visitors requiring access into the premises for official purposes shall approach the reception staff / security guards at the reception and shall need to identify themselves. They shall need to declare the purpose of their visit and shall then be granted access.

• **Zone 2**

- Work areas shall refer to areas that can be accessed only after a thorough verification of the identity of the individual and shall include the sections where the employees carryout their daily activities.
- Access to these areas shall be granted to individuals only for professional reasons and only once they have been duly identified.
- Entry to work area shall not by default entitle access to sensitive areas or restricted areas but shall only allow access to areas that can be accessed by all employees or long term contractors but not by the general public by default.
- Access to work areas shall be controlled by access cards (badges) or equivalent security measures. The access cards shall duly identify the individual and grant him / her access to the permitted areas based on the individual's job profile and responsibilities.
- Preferred mechanism for Zone 2 shall be automated access controls (for example, displayable badges combined with proximity based access control) for restricting access to work areas. In absence of an automated system, access to work area shall be controlled by way of security guards stationed at entry / exit points.

i. For Employees / Long Term Contractors

- All employees of RHFL entities and contract staff who are authorized to enter the premises on a long term basis shall be provided with Personalized

Identification Card access cards (badges) identifying them to the organization. Access to Premises shall be granted upon display of identification badges issued to the employee / long term contractors.

- Certain long term contractors shall also have individual access cards with their name and photograph printed on the face of the card. Other long term contractors will be issued General Purpose Long Term Cards.
- In general, access cards for Zone 2 shall not be transferrable. However, when required to be transferrable for contractors working in shift duties an offline record of the ownership of the card will be maintained in the shift entry register to establish accountability for usage of these cards.
- The badge holder shall be responsible for:
 - a. Using the badge to gain access to the controlled/secured zone
 - b. Wearing the badge noticeably
 - c. Not entrusting the badge to another person
 - d. Not using the badge to allow access to any other person (tailgating)
 - e. Surrendering the badge on expiry of the rights justifying its possession.

ii. For Service Providers / Entities Authorized To Enter For A Limited Period

- Service providers requiring access to the premises for official purposes for a period of more than a single work-day shall be issued General Purpose Long Term Cards with 'C' marked on them.
- Entities authorized to enter the premises for a limited period shall be issued visitor badges with 'V' marked on them.
- In both cases the period of grant of access shall be configured on the badge itself. In general the access shall be configured for the main entrance, the cafeteria and the floor that the contractor /other visitor shall need access to.
- Access to Premises shall be granted upon display of identification badges issued to the individual and in addition through appropriate configuration in the automated access control system, if implemented for contractors.

iii. For Visitors Authorized To Enter The Premises On A One-Time Basis

- All visitors requiring access to the premises on a one time basis shall be issued General Purpose One Time Visit Card. The visitors shall need to identify themselves and the purpose of their visit to the reception staff or security guards stations at the entry/exit to RHFL Premises. Access to work areas shall be granted to visitors as follows:
 - a. The reception/ Security staff shall make an entry of the visitor and capture details of the visitors such as name, Date & time of visit, , whom to visit

(host), purpose of visit, details of items carried such as laptops, mobiles, pen drives and other portable media.

- b. Upon identification and verification, the reception staff / guard shall verify the purpose of visit with the concerned staff, and provide the visitor with a temporary visitor pass.
 - c. Unless specifically requested and approved, this “V” card will be without Access rights.
 - d. The host shall be informed by the reception staff who shall escort the visitors into the areas as required.
- The responsibilities of the visitor shall include:
 - a. Wearing the badge noticeably
 - b. Not moving around in the company’s buildings without being accompanied by the host.
 - c. Surrendering the visitor pass / badge on exit once the purpose of the visit has been accomplished
 - The responsibilities of the host shall include:
 - a. Announcing his/her visitors in advance if already known
 - b. Requesting the appropriate physical access rights for his/her visitors
 - c. Escorting the visitor in and out of the premises and accompanying his/her visitors throughout their presence in the company’s buildings
 - d. Informing his/her visitors of the company’s rules relating to moving around in the premises
 - e. Ensuring that his/her visitors surrender their badges when the visit is over.
 - **Sensitive Areas (Zone 3 and 4)**
 - Sensitive areas shall refer to the areas that can be accessed only after a thorough verification of the identity and purpose of the individual. Access to these areas shall be extremely restricted and granted to individuals only on an absolute need basis.
 - Due to the nature of the activities performed in these areas or the tangible and intangible value of the assets stored in these areas the level of security controls implemented to access these areas shall be high.
 - Access to these areas shall be granted for strictly professional reasons. Visitors shall not have access to these areas unless required for business purposes
 - Preferred mechanism for access to sensitive areas shall be the use of an automated access control system. In absence of automated access control assets in sensitive areas shall be secured by the use of lock and key. In absence of an automated system or lock

and key, access to sensitive area shall be controlled by way of security guards stationed at entry / exit points.

- Access shall be granted only on an absolute need basis. For anyone other than the individuals authorized to access the sensitive areas, on a perpetual basis, due to the nature of their work, an explicit approval shall be required from the designated sensitive area owner.

- i. For Employees / Long Term Contractors

Employees or long term contractors who need to have access to these areas due to the nature of their work shall be granted access to these areas using access badges. The access badges of such employees and contractors (typically technical maintenance staff etc.) shall be configured to grant them access to these areas. The access rights for such individuals shall be reviewed by the designated manager / secured area owner on a half yearly basis to ensure that the access rights remain as required.

- ii. For Service Providers

Service providers requiring one time access to the sensitive area shall have to identify themselves at the reception. Upon identification and an explicit approval shall be required from the designated sensitive area owner they shall be granted temporary access pass. The service providers shall be escorted throughout their duration of visit by an employee authorized to enter the sensitive area.

- iii. For Visitors

Visitors shall not be granted access to the sensitive areas. Any exceptions to this shall require an explicit approval from the designated sensitive area owner. Also any such cases shall need to be escorted throughout their visit to the sensitive areas by an employee authorized to enter the sensitive area.

2.13.3.3 Environmental Standards for Zones

Environmental security controls shall be implemented by RHFL to protect its People and Infrastructure from physical and environmental threats. The protection of the People and Infrastructure is essential for the overall effectiveness of the overall security support structure. This policy shall ensure that appropriate measures are taken to safeguard the People and Infrastructures from incidents such as fire, flood, electrical supply, temperature extremes and earthquakes.

The administration teams shall be responsible for the design and implementation of environmental controls and the BISO shall be responsible to ensure their adherence and compliance.

- **Zone 1**

- Buildings shall have minimal points of entry to avoid unauthorized personnel gaining access to building
- Fire exits shall not be locked and shall have one way crash bar, easy opening mechanism and where possible trigger an appropriately loud alarm when opened to

prevent misuse of the same. If it is locked key shall be provided next to it in Breakable Glass box, which can be used by the employees for opening the door in emergency situation.


- Buildings shall have appropriate lightning protection which shall be tested on periodic basis
- Buildings shall have a backup power source to continue minimum necessary operations. The preferred mechanism for the same shall be installation of DG sets in case of power failure. Where feasible, a UPS power backup shall be installed for critical resources to provide uninterrupted power supply in case DG sets are not operational.
- A technical team shall be available to monitor environmental parameters / respond to anomaly reported by the monitoring staff particularly if the anomaly pertains to server rooms / data centers.

- **Zone 2**

- Work Areas shall be accessed through access control cards to restrict unauthorized entry of any personnel
- Work areas shall be monitored for any leakage or any water intrusion
- Work areas temperature shall be monitored by the monitoring staff and administered by a person in charge
- Work areas shall have sufficient number of fire exit points and employees shall be given training of fire evacuation procedure in case of emergency (Refer to Evacuation Procedure Manual). Evacuation drills shall be performed at least on an annual basis.
- Fire extinguishers shall be positioned at each floor. ERT members present at every floor shall be trained to operate the fire extinguisher in case of any emergency situation
- Work areas shall have smoke detectors positioned all over to detect any instance of fire and give warning alarm immediately
- Floor plans shall be displayed at specific locations on each floor
- Employees are expected not to carry inflammable items

- **Environmental Security For Sensitive Areas (Zone 3 And Zone 4)**

- Sensitive areas shall be protected from any water leakage and will be monitored by the BMS team
- Smoke detectors shall be positioned to detect any instance of fire
- Alarms and Intrusion detection systems shall be installed to notify of any unwanted object/personnel. All physical intrusions shall be treated at par with information

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

security breaches and thus be investigated accordingly. Corrective and punitive action shall be taken and promulgated to all in case of such an intrusion / breach.

- Sensitive areas (Data Centers, Server Rooms) shall have appropriate fire prevention equipments installed. Preference shall be given to automated fire detection and suppression equipments. Sensitive areas shall have fire resistant doors, walls to safeguard against fire damage
- Temperature for sensitive areas shall be monitored more frequently. Sensitive areas shall have proper electricity backup

2.13.3.4 Security in Transit

- Appropriate measures shall be implemented by RHFL to enable secure transit of information assets stored in Zone 3 or 4.
- RHFL equipment, data or software must not be taken off-site without proper authorization.
- Provision for safe exchange of information assets shall be considered at all times.
- The transportation facility shall be managed by a service provider contracted and approved by RHFL.
- Employees and security personnel shall be expected to adhere to the guidelines provided and be equally responsible to ensure the safety of the assets during the transfer.

2.14 Monitoring, Logging and Assessment

2.14.1 Purpose

To define the RHFL desired practices regarding monitoring, auditing and assessment of logs.


2.14.2 Scope

This policy applies to all information systems information assets and all communication and network connections through which RHFL Information Assets are transmitted, stored or processed. Information systems, communications and network connections include, but are not limited to, network devices such as routers and firewalls, servers and mainframes all operating systems, databases and applications.

2.14.3 Policy

All critical information systems deployed by RHFL for information processing, storage or security shall be monitored through the following means:

- Real time monitoring through manual means or technology systems capable of generating alerts.
- Logging of all activities or transactions performed on information systems and periodic analysis of logs.
- Periodic or one-time security posture assessment exercises including but not limited to device configuration review, security testing of information systems and review of IT processes set up for real time or periodic monitoring.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

Any breach of this policy shall be considered as an incident and shall be treated as per the incident management policy.

2.14.3.1 Logging and Monitoring

All information systems shall be classified based on the asset management policy and monitoring processes shall be set up as below:

- Real-time automated detection facilities shall be implemented for systems to monitor significant deviations from normal activity and to alert security administrators of those systems.
- Logging shall be enabled for all business transactions, high risk systems and processes shall be set up for real time or periodic manual or automated review of logs.
- Logging shall be considered and implemented based on performance implications for low-risk systems and processes shall be set up for periodic review of logs.


2.14.3.2 Physical access and activity

- Zone 1
 - A register shall be maintained of all the individuals/ visitors, except employees, with their name, contact, purpose and their timings to facilities.
 - Close circuit television (CCTV) cameras shall be installed at all entry points for critical facilities. The monitoring of these visuals shall be done by authorized personnel.
 - The video tape recording shall be maintained as per the stipulated guidelines, statutory requirements.
- Zone 2
 - CCTV cameras shall be installed at all strategic entries and exit for critical facilities. The visuals shall be monitored at periodic intervals, by the authorized personnel.
 - The video tape recording shall be maintained as per the stipulated guidelines, statutory requirements.
 - Temperature for the work areas shall be monitored and action taken for deviations from set standards.
 - Electrical supply shall be monitored by the sub contractor engaged for the premises.
- Zone 3 and Zone 4
 - Parameters such as temperature and humidity of the data centers shall be monitored closely / more frequently. The authorized personnel shall manually log the temperature of the data centre every two hours.
 - CCTV cameras shall be positioned in the sensitive areas unless prohibited by law and shall be monitored by the authorized personnel at periodic intervals.

- The video tape recording shall be maintained as per the stipulated guidelines, statutory requirements. Water leakage shall be monitored by the sub contractor.
- Day to day operations, maintenance and monitoring of AC / Power supply and other environmental controls can be sub-contracted to vendors. However the final responsibility and authority for the same shall remain with RHFL.
- Records of monitoring such as registers/ logs shall be maintained by the sub contractor.
- Annual maintenance contracts (AMC) shall be in place for critical equipment with OEMs (Original Equipment Manufacturer) for periodic /preventive maintenance and support during breakdowns.
- Pest Controls shall be done on need basis to avoid any damage by the rats and rodents

2.14.3.3 Information systems logging and monitoring

- All information systems will be configured to log system activities and generate alerts for any unusual activity to system administrators.
- The activities of privileged users such as system administrators and system operators shall be logged and independently reviewed on a regular basis.
- Mechanisms shall be put in place to detect and report activity which violates the Information and Cyber Security Policy with respect to access, acceptable usage and / or any other aspect addressed by the policy.
- In absence of automated alerts, a process shall be set up to perform manual review of activity logs, on a frequency defined based on the criticality of the information system.
- The clocks of all relevant information processing systems within RHFL or security domain shall be synchronized with an agreed accurate time source
- The IS Operations team responsible for monitoring the network equipment and network activity shall analyze the alerts and logs and any activity requiring action shall be raised as incidents as per the incident management policy before taking such action except in emergencies.
- Where the action to be taken requires changes to the information system configurations, such changes shall be subject to the change management policy.
- The activity logs shall be retained based on the record retention requirements.
- Logging facilities and log information shall be protected against tampering and unauthorized access.
- **Network access and activity**
 - All communication to or from external networks shall be logged and the logs reviewed periodically or real time automated monitoring mechanisms shall be established for the purpose.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- Mechanisms such as internet access filters shall be set up for adherence to acceptable usage policy of RHFL with respect to access to external networks; and the same shall be monitored and reviewed.
- **Application access & activity**
 - User activities, exceptions, and security events on all applications shall be logged and monitored. Logs must include the following:
 - System starting and finishing times
 - System errors or Faults and corrective action taken
 - Confirmation of the correct handling of critical data files and computer output.
 - The name of the person/process / system making the log entry
 - Source address from where data or system is being accessed (this might be either IP address or MAC ID)


2.14.3.4 Transfer and Movement of assets

RHFL shall either transfer assets from one RHFL entity to the other or move them in and out of RHFL facilities when either being procured or sent for destruction.

Procedures shall be developed for entry /exit to and from RHFL premise regarding new assets which have been procured or assets which are sent to the vendor premises for repair / sent for destruction / sale

2.14.3.5 Information Security assessment

- **Security assessments for infrastructure and applications**
 - The IS team will define guidelines for conducting Vulnerability assessments and security review of infrastructure. The guidelines shall include:
 - Frequency of conducting assessments based on criticality of applications
 - Coverage of security assessments
 - Approach (internal vs. external) for conducting security assessments based on criticality of applications
 - Network and application vulnerability assessments shall be performed on an ongoing basis by competent personnel. The risks identified shall be documented in the assessment report.
 - The results of the assessment report shall be analyzed and acted upon by the team responsible for maintaining required the information system.
 - All security assessments reports and the actions taken shall be reviewed by the Information security team.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- Risks identified through security assessments which remain unmitigated due to technology limitations or business requirements shall be highlighted to the notice of the ISRMC for resolution or exception approval.
- **Internal IS assessment by IS Team**
 - RHFL shall conduct annual review of information security practices either by the IS team or by competent independent party appointed by the IS team to ensure compliance with the information security policies, procedures and internal guidelines defined by the IS team.
 - Formal procedures shall be developed by the IS team for planning and reporting of reviews findings and ensuring the implementation of a prompt and accurate remedial action.
 - Annual Information Security Audit to cover branches
- **External IS assessment**
 - RHFL shall conduct formal external IS reviews by competent independent party to ensure compliance with the information security policies, procedures, external industry standards as per frequency defined by the Internal Audit team.
 - Formal procedures shall be developed by the Internal Audit team for planning and reporting audits and audit findings and ensuring the implementation of a prompt and accurate remedial action.
 - The Internal Audit Team shall be responsible for defining the scope of the review and coordinating with the business and support teams.
 - Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.
 - External assurance audit every financial year

2.15 Cloud Security

2.15.1 Purpose


To define the RHFL desired practices regarding Cloud Security.

2.15.2 Introduction

Cloud Computing has become a ubiquitous concept in Information Technology arena and is widely agreed to be the key to future of IT. National Institute of Standards and Technology (NIST) has defined cloud computing as:

“Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

As per the NIST, there are five essential characteristics of cloud computing, which are:

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- On demand self-service i.e. provisioning of additional computing facilities without human intervention
- Broad network access i.e. accessibility from a variety of devices
- Resources pooling i.e. sharing of infrastructure like data center, hardware, infrastructure software and application software.
- Rapid Elasticity i.e. resources allocated can grow or shrink dynamically depending upon load and
- Measured service i.e. pricing would be based on actual usage rather than cost of equipment.

Cloud computing needs to satisfy these five essential characteristics, use one of the four service models (section 2.15.5.1), and deploy using one of the three models (section 2.15.5.2).


2.15.3 Scope

This policy applies to all business functions and its information systems, information assets and all communication and network connections that use or plan to use cloud computing services or cloud infrastructure services. Information systems, communications and network connections include, but are not limited to network devices such as routers and firewalls, servers and mainframes and operating systems, databases and applications.

- Data
- Application
- Functions
- Process
- Network connections
- Underlying Hardware

The assets are to be evaluated on the following factors:

- Determine how important the data or function is to Reliance Home Finance
- Analyze the impact of the scenarios:
 - The asset becoming widely public and widely distributed
 - An employee of the Cloud service provider accessing the asset
 - The process or function being manipulated by an outsider
 - The process or function failing to provide expected results
 - The information/data being unexpectedly changed
 - The asset being unavailable for a period of time

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

2.15.4 Role and Responsibilities

- **Cloud Consumer**

- This shall be the entity that, avail the services of the cloud. For RHFL, the cloud consumer shall include all its group companies. Cloud consumers shall:
 - Retain ownership of, and rights to use, their own data.
 - Ensure that the cloud vendor lives up to its SLAs and controls within the service agreement. They shall also ensure that the vendor meets certain obligations around security, privacy, data ownership, uptime, performance, and more
 - Perform due diligence of the cloud service provider before onboarding.
 - Comply with the Information and Cyber Security Policy, procedures and guidelines of RHFL.


- **Cloud Service Provider**

- Cloud service providers (CSP) offer network services, platform, infrastructure, or business applications in the cloud. The cloud services are hosted in a data center that can be accessed by companies or individuals using network connectivity.
- CSPs are responsible for implementation and maintenance of information security controls across the services they provide.
- CSPs shall comply with the Information and Cyber Security Policy, procedures and guidelines of Reliance Home Finance

2.15.5 Policy

The objectives of this policy are:

- To ensure that the cloud service is in accordance with the business and security requirements and relevant laws and regulations for:
 - Provisioning and Commissioning of Cloud Services.
 - Operations and Management of Cloud Services.
 - De-commissioning of Cloud Services.
- To evaluate the following factors in cloud adoption decisions:
 - Technical adequacy for porting the application to the Cloud – Assess the application profile to ensure it is a right fit to be ported to the Cloud.
 - Risk including availability requirements, regulatory, compliance and statutory requirements, data sensitivity.
 - Control over intrusion decisions, vulnerability monitoring, denial of service attacks.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

Any deviation from this policy shall be treated through risk management and exception management as defined in the IS policy: General policies, section 1.7 Risk management and Section 1.8 Exceptions.

2.15.5.1 Cloud Service Models

Cloud service delivery is divided among Four archetypal models

- **Cloud Software as a Service (SaaS)**
 - The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure.
 - The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email).
 - The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.
- **Cloud Platform as a Service (PaaS)**
 - The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider.
 - The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
- **Cloud Infrastructure as a Service (IaaS)**
 - The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.
 - The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of selected networking components
- **Business Process as a Service (BPaaS)**
 - The capability provided which includes, business process outsourcing (BPO) services that are sourced from the cloud and constructed for multi tenancy.
 - The Services are often automated, and where human process actors are required, there is no overtly dedicated labor pool per client.

2.15.5.2 Cloud Deployment Models

- **Public Cloud**
 - Cloud infrastructure owned and operated by a third party organization selling cloud services and available on a rental basis to the general public or a large industry group

- **Private Cloud**

- Cloud infrastructure is owned and operated solely for a single organization. It may be managed by the organization or a third party, and may exist on-premises or off premises.

- **Hybrid Cloud**

- Cloud infrastructure is a composition of two or more different cloud infrastructures (private, community, or public) that remain separate entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., load balancing between clouds).

2.15.6 Compliance

Reliance Home Finance shall ensure compliance with various National Housing Bank (NHB) guideline and related laws, regulations and guidelines issued by the regulating authority in India as applicable.

2.15.7 Cloud security lifecycle

Governance and risk management, while the deployment model may define accountability and expectations.

Reliance Home Finance shall ensure before signing an agreement with the cloud service provider, to the complete approval of all the mandatory controls

2.15.7.1 Authentication


- It shall be ensured that the Cloud Service Provider supports various Multi-factor authentication mechanisms.
- Authorization shall be followed as per the existing “Information and Cyber Security Policy, Security Domain Policy, Section 2.2 – ‘Asset management’, subsection 2.2.3.2 Lifecycle Processes - Authorization Inventory.
- Reliance Home Finance shall affirm that the cloud service providers authentication process, access control, accountability and logging are in line with applicable regulatory and legal requirements.
- Customer data shall be protected from any unauthorized access.

2.15.7.2 Physical Security Controls

The Physical Security Controls shall be followed according to the existing “Information and Cyber Security Policy, Security Domain Policy, Section 2.13 – ‘Physical and Environment Security’”.

The additional physical security controls are mentioned as follows:


- Reliance Home Finance shall ensure that the Cloud Service Provider complies with the appropriate security controls of the infrastructure. Effective physical security shall ensure that centralized management system allows for correlation of inputs from various sources, including property, authorized employees.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- It shall be recommended to opt for Cloud service providers that conform to the ISO 27002 standard for physical and environmental security.

2.15.7.3 Infrastructure and Network Security Controls

- Infrastructure Security (for private cloud and IaaS for public cloud)
 - Design of the Cloud environment shall be based on appropriate security guidelines such as Cloud Security Matrix by Cloud Security Alliance or as per guidelines defined by IS Team. The IS team shall perform an assessment of private Cloud services prior to roll out based on industry standards and IS policy provisions.
 - An infrastructure standard shall be defined and implemented for commissioning of cloud infrastructure including servers and network equipment. The standard shall consider legacy infrastructure or provision for reuse or retiring the same if required. The standard shall also include minimum security baseline standard.
 - Appropriate tools / procedures shall be put in place for managing and monitoring infrastructure operations including Cloud characteristics such as storage utilization, provisioned allocation vs. actual utilization, host machine uptime, virtual machine uptime, network uptime and infrastructure and application response times, patch management, change management, incident management, antivirus management.
 - Infrastructure integration architecture shall be defined for integration within the data center and across multiple data center.
 - All applications and infrastructure elements shall be evaluated for their suitability to operate on the Cloud environment prior to migration, including checks for compatibility and information security baseline. A procedure document shall be made available for performing such a migration. Necessary approvals from Security and Business shall be obtained at various stages during migration as defined in the existing “Information and Cyber Security Policy, Security Domain Policy, section 2.5 - Information Systems acquisition and development. Cloud infrastructure shall follow the existing RHFL’s Information Systems Maintenance policy including access control, change management, Data security, backup and restoration, patch management, job scheduling, capacity and performance management, malicious software management, vulnerability management, and IT service management.
- Network Security
 - Network security consists of security services that restrict or allocate access and distribute, monitor, log, and protect the underlying resources services.
 - It shall be followed according to the existing “Information and Cyber Security Policy, Security Domain Policy, Section 2.9. ‘Network Security’”.
 - Also, Reliance Home Finance shall ensure that the cloud service provider has documented and tested processes for:
 - Access controls, for management of the network infrastructure
 - Traffic filtering, provided by firewalls

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- Creating secure Virtual Private Networks (if VPN is offered)
- Intrusion detection / prevention
- Mitigating the effects of DDoS (Distributed Denial of Service) attacks
- Logging and notification, so that systematic attacks can be reviewed.

2.15.7.4 Data Isolation

- In case of utilization of cloud services, Reliance Home Finance shall ensure that its data is adequately isolated in the cloud environment.
- RHFL’s data on the cloud shall be isolated such that it can operate as a separately managed entity/entities.
- Mechanisms shall be established to ensure appropriate isolation exists at the network, operating system, application layer and database.
- For a multi-tenant cloud environment, the following shall be ensured:
 - Mechanisms shall be defined for separating the usage of storage, memory, and routing. The isolation of applications and data shall be ensured. In an isolated architecture, the data shall be segregated into its own database instance. For multi-tenancy, an architectural and design approach shall be adopted to economies of scale, availability, management, segmentation, isolation, and operational efficiency.
 - For the application deployed on the Cloud using native multi-tenancy features offered by the application, privacy of data across tenants or entities shall be ensured through appropriate access control mechanisms. Application shall clearly log business errors and technical errors separately to support separation of duties between business users and data center operator.

2.15.7.5 Data Classification

Data Classification shall be followed in accordance with the existing “Information and Cyber Security Policy, Security Domain Policy, Section 2.1 – ‘Data Classification’”.

2.15.7.6 Encryption

- As defined in the existing “Information and Cyber Security Policy, Security Domain policy, Section 2.10 – ‘Cryptographic Controls’”, Reliance Home Finance shall ensure that appropriate cryptographic controls are applied to data depending upon its classification as per encryption requirements defined in the data classification policy.
- Reliance Home Finance shall ensure that a unique set of encryption key(s) are utilized, in accordance with the existing “Information and Cyber Security Policy, Security Domain Policy, Section 2.10 – ‘Cryptographic Controls’, subsection 2.10.3.2 – ‘Key Management’”.
- Reliance Home Finance shall ensure that the cloud service provider support Key Management Interoperability Protocol (KMIP). KMIP provides a standardized way to manage encryption keys across diverse infrastructures.

- Reliance Home Finance shall prefer Hardware encryption keys, in compliance with the Federated Information Processing Standard (FIPS) 140 2-3 and above, whenever compatible.
- Reliance Home Finance shall devise encryption, key management procedures in accordance with the already existing RHFL's Information and Cyber Security Policy for the following:
 - To encrypt data in transit, at rest, backup media
 - To Secure key store
 - To protect encryption keys
 - To ensure encryption is based on industry/ government standards
 - To Limit access to key stores
 - Key backup and recoverability
 - To test these procedures

2.15.7.7 Application Security

Reliance Home Finance shall ensure Application Security for applications hosted over the Cloud in accordance with the existing "Information and Cyber Security Policy, Security Domain Policy, Section 2.5 – 'Information Systems acquisition and development', subsection 2.5.3.1. Technology Standards– Application Security.

2.15.7.8 Incident Management

The incident management for cloud services shall be followed in accordance with the existing "Information and Cyber Security Policy, Security Domain policy, Section 2.8 - 'Incident and Problem Management'".

2.15.7.9 Business Continuity and Disaster Recovery

- Reliance Home Finance shall ensure Business Continuity for cloud services shall be in accordance with the existing "Information and Cyber Security Policy, Security Domain Policy, Section 2.11 – 'Business Continuity Management'".
- In addition, Reliance Home Finance shall also audit the Cloud service provider's disaster recovery plan and ensure it meets RHFL's requirements. At minimum, the following shall be considered:
 - The ability to retrieve and restore data following data loss incidents.
 - The cloud service provider shall provide Reliance Home Finance a disaster recovery testing report that would be extensive, covering from exercise scope to the final outcome and recommendations.
 - Make sure the DR (Disaster Recovery) solution is capable of maintaining the same levels of security measures and controls utilized in normal operation mode.
 - Assure that the Disaster recovery solution is owned and managed completely by the contracted Cloud Service Provider.

- It is recommended to opt for cloud service providers who are BS25999 or ISO 22301 certified.
- Business Continuity Plans shall be in place for cloud sourced services based on regular BCP and provisions for the same shall be included in Reliance Home Finance contracts.
- A confidential document containing account information for business continuity purposes shall be maintained

2.15.7.10 Exception Management

- An “exception” shall be defined as circumstances when a particular policy or standard; security program requirement; or security best practice cannot be fully implemented.
- Reliance Home Finance shall develop, publish and implement administrative, technical and physical safeguards in an effort to adequately protect the confidentiality, integrity and availability of its assets on an exception basis.
- The Exception Management for Cloud Services shall be followed in accordance with the existing “Information and Cyber Security Policy, General Policy, Section 1.8 –“Exceptions””.

2.15.8 Offboarding of cloud service provider

- Upon termination of contract, all data transferred by RHFL, or generated by the third party for RHFL, shall be handed over to RHFL. Evidence shall be provided to RHFL for deletion and purging of all copies of data at service provider site/s
- When in transit, data shall be subject to stringent controls based on the classification of data as laid down in the Information and Cyber Security Policy: Security Domain Policy, Section 2.1 – ‘Data Classification’.
- Upon termination of services, the service provider shall provide a certificate to ensure that de-commissioning has been carried out and further access shall not be provided to Reliance Home Finance employees.


2.15.9 Virtualization

In cloud computing, majority of logical separation controls are not physical, it is enforced through logical system and application controls designed to help ensure data segmentation and integrity across the platform. The mechanism for providing this separation of data and services is “virtualization”.

2.15.9.1 Evaluation of Cloud Service Provider virtualization environment

Reliance Home Finance shall evaluate the Cloud service providers’ virtualization hardening guidelines and policies and evaluate the third party gap assessment against technology risk assessment checklist. This includes but not limited to:

- Disable or remove all unnecessary interfaces, ports, devices and services;
- Securely configure all virtual network interfaces and storage areas;
- Establish limits on VM resource usage;

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- Ensure all operating systems and applications running inside the virtual machine are hardened;
- Validate the integrity of the cryptographic key- management operations;
- Harden individual VM virtual hardware and containers;

2.15.9.2 Virtualization Security

Reliance Home Finance shall ensure that the Cloud security provider has controls to guarantee that only authorized snapshots/ images are taken and that these snapshots/ images' level of classification, storage location and encryption is in compliance with the production virtualization environment.

Reliance Home Finance shall assure the following controls are applied as a part of hypervisor security:

- Reliance Home Finance can access the Hypervisor administrative access log reports.
- Hypervisor complete logging is enabled.

Reliance Home Finance shall ensure that the cloud service provider gives assistance of trusted Virtual Machines (VM) and those VMs were made in compliance with the hardening guidelines.

The cloud service provider shall provide Reliance Home Finance with its complete vendor list that will have access to RHFL's data; at any point throughout the duration of the agreement. The Cloud Service Provider shall update Reliance Home Finance about any change in the vendor list.

For multi-tenancy through virtualization,


- Application shall be explicitly tested and qualified using virtualization product that is deployed within the Cloud. Application vendor shall provide sizing considering deployment under virtualized environment. Alternatively vendor shall provide sizing based on physical servers and state the overhead with specific virtualization product.
- Application image shall be available for the virtualization product used. Each virtual machine shall be allocated resources commensurate with projected transaction. Resource consumption shall be periodically monitored against actual load so that necessary refinements can be carried out.

Putting different tiers of the application onto separate physical boxes shall allow passing communication between tiers to go through physical network and facilitate implementation of firewall policies to allow communication only between VMs belonging to the same company. Also, using different disk partitions to isolate VMs belonging to different companies can provide further isolation.

2.15.10 Legal, Regulatory and Contractual Requirements

2.15.10.1 Contractual Requirements

Reliance Home Finance shall sign a non-disclosure agreement (NDA) with the cloud service provider before providing any service. All aspects relating to privacy, confidentiality, security and business continuity shall be fully met.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

If the vendor is certified under the Cloud Security Alliance Trust or is providing control information under the Cloud Trust Protocol, and if the scope of services provided to Reliance Home Finance is included under the scope / statement of applicability for the certification, the vendor shall be exempt from the requirement for periodic audits by RHFL. However, in such a scenario, the vendor will be required to furnish the following:

- A self-certificate of compliance to all IS provisions in the contract
- Copy of a valid certifications demonstrating that the scope of services provided to Reliance Home Finance is included under the scope / statement of applicability for the certification
- In order to be able to enforce performance, information security and other controls to address outsourcing risks, Reliance Home Finance shall build the right to audit as part of contract with vendors.

Information Security department shall be engaged during the establishment of Service level agreements (SLAs) and contractual obligations to ensure that security requirements are contractually enforceable.

Reliance Home Finance shall prepare a service contract addressing the following domains:


- Architectural Framework
- Governance, Risk Management
- Clarity on Cloud service provider’s role and RHFL’s role
- e-Discovery searches
- Expert testimony
- Primary and secondary(logs) data
- Location of storage
- Contract termination
- Ownership of data

Reliance Home Finance shall ensure that the Service Level Agreement(SLA) reflect the applications and data availability requirements in the occurrence of planned or unplanned disruptions or outages, business continuity and disaster recovery planning and backup and redundancy mechanisms defined by RHFL.

Reliance Home Finance shall include the financial remedies in the event of a business disruption in the SLA.

Third party service providers shall be empanelled for the cloud services of Reliance Home Finance only after a contract is signed between Reliance Home Finance and the service provider.

The contracted terms and condition shall be approved and drafted by the Legal department of Reliance Home Finance for safeguarding the interest of Reliance Home Finance in consultation with Compliance, Risk and Information Security departments.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

Automated tools shall monitor and track SLA's and generate reports to project the impact on costs, ROI etc.

The provisioning process shall be completely automated.

2.15.10.2 Contractual clauses on Data Privacy

Reliance Home Finance shall assure that it retains the “Exclusive” right to data ownership throughout the duration of the agreement. Ownership includes all copies of data available with cloud service provider including the backup media copies, if any. Reliance Home Finance shall ensure that the cloud service providers are not permitted to use RHFLs’ data for advertising or any other non-authorized secondary purpose.

Reliance Home Finance shall contractually assure that they are informed of any confirmed breach immediately without any delay. For suspected breach, Reliance Home Finance shall be informed within 4 hours from the time of breach discovery.

Reliance Home Finance shall contractually require that the cloud service provider be responsible for any financial losses or penalties that may occur in event of a cloud service provider breach.

Reliance Home Finance shall contractually require that the cloud service provider will completely eliminate any trace of data/ information at the termination of the Contract as agreed in the contract.

Reliance Home Finance shall contractually require and ensure that the cloud service provider will fulfill the data and media destruction and sanitization controls.

Reliance Home Finance shall ensure that the cloud service provider complies with the requirement of return of data to Reliance Home Finance. There shall be no Vendor-lock in by the cloud service provider.

2.15.10.3 Legal Requirements

Reliance Home Finance shall ensure that the Cloud service provider’s own data privacy policy is in compliance with the applicable laws in RHFL. Also, the cloud service provider shall adhere to all regulatory and legal requirements of the country.

Data and processes in Cloud Computing shall comply with both Indian and international laws when Reliance Home Finance availing the Cloud service has an international presence. Legal compliance shall be ensured when using the Cloud service.


2.15.10.4 Regulator Independence

Reliance Home Finance shall contractually agree with the cloud service provider that the infrastructure and applications are made available for audit/ inspection by the regulators of the country. Regulator shall have access to all information resources that are consumed by RHFL, though the resources are not physically located in the premises of RHFL.

2.16 BYOD Security

2.16.1 Purpose

The Bring Your Own Device (‘BYOD’) Policy governs the use of employee owned devices (e.g. tablets, smart phones/ equivalent) for accessing corporate emails, applications and data.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

The purpose of this policy document is to:

- Define employee eligibility for using personal-owned smart phones/tablets to access corporate data
- Define the responsibilities, guidelines, and terms of use for personal-owned devices.

This policy has been defined under the provisions of the Reliance Home Finance Information security policies as referred in various sections below. However, in the event of any conflict between this policy and the information security policies, the CISO shall be responsible for resolution of the same; Refer to 'General Policy: 3.0 Governance'

- Ownership and interpretation' for further information.

2.16.2 Policy Statement

2.16.2.1 Eligibility and Ownership

- All full time employees shall be allowed to configure their personally owned devices for corporate email, application and data access (BYOD program) through Mobile Device Management solution only.
- Contractors or third party employees can enroll their personal devices under BYOD program through Mobile Device Management solution only after due management approvals (on case to case basis).

2.16.2.2 Device Scope


- RHFL's IT function shall maintain a 'white-list' of device models, which can be configured under the BYOD program, as per the technology compatibility and security considerations. This list would be updated by IT function periodically.
- RHFL shall support devices with following OS platforms but not limited to -
 - Android - OS version 2.3 and above
 - Apple - iOS version 4 and above
 - BlackBerry - OS version 5 and above
 - Windows - OS version 8 and above

2.16.2.3 Device Setup

RHFL's IT functions would setup a self-configuration portal for BYOD enrollment. Eligible employees shall be provided access to this portal to setup and configure their devices. RHFL's IT function shall support in configuration in case of any issues

2.16.2.4 Ongoing Support and Device Maintenance

- RHFL's IT functions shall provide support for corporate applications and corporate data on devices enrolled as part of BYOD program.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- RHFL's IT functions would not own the support for managing employee's personal device hardware/ non-corporate software issues.

2.16.2.5 Employee/ Device Exit Process


- In case of employee resignation/ exit from RHFL – Refer to 'Security Policies: 10.04 Human Resource Security.'
- In case of absconding employee, HR shall inform IT function at the earliest. The latter shall perform remote wipe of corporate data from the device. In case the remote wipe is not possible, the same shall be reported as an Information Security incident as per 'Security Policy: 10.08 Incident and Problem Management'.
- In case of loss of device, the employee shall inform IT function within 4 hours. IT function shall perform remote wipe of corporate data from the device as per Annexure B as defined below. In case the remote wipe is not possible, the same shall be reported as an Information Security incident as per 'Security Policy: 10.08 Incident and Problem Management'.
- RHFL shall deploy appropriate information security controls on the devices enrolled under BYOD program to enforce appropriate access controls defined in the 'Security Policy: 10.03 Access Control.'
- This may include installation of a Mobile Device Management (MDM) tool.

2.16.2.6 Periodic Audit & Non Compliance Remediation

IT function will be authorized to monitor or periodically review the device configurations (as per the 'General Policy: Acceptable Usage – (II). Acceptable usage of personal devices for official purposes. Point (c)' to identify any exceptions to RHFL's policies. The monitoring and logging of activities on the mobile device shall be performed in compliance with 'Security Policy: 10:14 Monitoring, Logging and Assessment'.

2.16.2.7 Annexure

- **Annexure A – Key Definitions**
 - Data Classification
 - Corporate Data – means applications and data belonging to RHFL or its affiliates, including but not limited to emails, calendar, contact data, corporate applications, documents, images etc. The same shall be classified as per the 'Security Policy: 10.01 Data Classification.'
 - Personal Data – any data/ applications other than Corporate Data, present on the employee's device
 - Device Type
 - Smart Phone – is a mobile phone built on a mobile operating system, with more common features of a handheld computer/ PDA and with more advanced computing capability and connectivity than a feature phone.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- Tablet – is a wireless, portable personal computer with a touch screen interface. The tablet form factor is typically larger than a smart phone.
- Mobile Device Management (MDM) – refers to specialized software intended to distribute mobile applications, data, configuration settings and implement IT Governance in mobile devices, including mobile phones, Smart phones, and tablet computers. The intent of MDM is to provide real-time management capabilities including convenient configuration, self-service and robust security while minimizing cost and downtime

- **Annexure B – Security of Personal Devices**

Following minimum security controls shall be configured on the personal devices having access to corporate data:

- Device Security


- Device Pass-code: Access to devices shall be protected by either a 4 digit device pass code or pattern recognition system. The corporate data on device shall be automatically wiped after 10 unsuccessful logon attempts.
- Access to RHFL applications / data: As defined in the ‘Security Policy: 10.03 Access control’, access to all RHFL application and/or data will be based on two-factor authentication.
- Device Locking: The device shall be locked after 5 minutes of inactive time.
- Device Tracking: To determine the location of an employee’s handset, devices shall be installed with software to track the same.
- Remote Locking: In the case of a lost or stolen phone or tablet, employees or RHFL’s IT function shall be able to remotely lock or, erase the specified device.
- Jailbreak Detection: Detection tools shall be installed in the devices to perform a comprehensive search for evidence that the built-in system protections on the device have been disabled.

- Data Security

- Remote Data Wipe: Devices enrolled under this policy shall be configured for remote erase capability through appropriate means such as an MDM software
- Data Encryption and Containerization: Please refer to ‘Security Policy: 10.10 Cryptographic Controls.’
- Application Blacklisting: RHFL’s IT function shall maintain a list of applications that are to be denied system access and shall prevent them from installing or running.

- BYOD Acceptable Use Policy

Refer to ‘General Policy: Acceptable Usage – (II). Acceptable usage of personal devices for official purposes.’

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

2.17 Cyber Security

2.17.1 Purpose

The varied challenges presented by cyber risk should be met with a broad response. Appropriately high-level management's attention is a necessity, as is an effective governance structure able to understand, prevent, detect, respond to, and address Cyber security incidents.

To provide guidelines for addressing cyber security and related risks and the mitigation of such risks.

2.17.2 Scope

This policy applies to information systems, including IT applications, IT infrastructure and physical information channels, information assets that RHFL uses, business processes and procedures.

2.17.3 Policy

The objectives of this policy are to:

- Prevent occurrence and recurrence of cyber incidents by implementing security proactive measures.
- Create infrastructure for conformity assessment and certification of compliance to cyber security best practices, standards and guidelines
- Create mechanisms for security threat early warning, vulnerability management and response to security threats
- Create processes, structures and mechanisms to generate necessary situational scenario of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions.
- Promote and launch a comprehensive awareness program on security of cyberspace.


2.17.3.1 Classification

- Critical Systems and Cyber Security Incidents shall be classified based on criticality and severity
- Threat wise detail classification guideline shall be defined as a part of Incident Management Procedure for Cyber Security Incidents
- Scoring model shall be defined to find out overall risk score

2.17.3.2 Cyber Resilience program

Cyber resilience is ability to continuously deliver the intended outcome despite adverse cyber events. Well-functioning cyber security management program consistent with cyber resilience best practices shall be in place and verified through supervisory review.


To be effective, cyber security needs to be addressed at all levels. Cyber security management program includes on-going processes and control improvements, incident management procedures such as response and disaster recovery, state-of-the-art network policies and procedures, rigorous management and control of user privileges, secure configuration guidance, appropriate malware

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

protection procedures, consistent control of removable media usage, monitoring of mobile and home working procedures, and ongoing awareness and educational initiatives for all personnel

Best practices for cyber resilience should include but not limited to below key areas:

- Identification
- Protection
- Detection
- Response and Recovery
- Testing
- Learning and Reporting
- Situational Awareness
- **Identification**
 - RHFL shall establish and follow a cyber threat intelligence process, analysis and information sharing process including but not limited:
 - The following Cyber threats shall be identified:
 - That could affect the operational performance
 - Cause significant impact to meet RNLIC^{''} objectives and obligations
 - Cause threat to critical business, processes and reputation
 - Necessary steps shall be taken to identify assets that need to be protected on priority.
 - Critical assets, business functions and processes shall be identified that shall be protected against compromise.
 - Information assets (including sensitive personal information) and related system access shall be part of the identification process.
 - RHFL shall establish a process to gather and analyze cyber threat information in conjunction with internal and external business and system information sources
 - Business process or Vendor risk shall be identified and assessed as a part of on-boarding and operations process.
 - For detail classification "Asset Management" section of "Information and Cyber Security policy" shall be referred.
- Protection
 - Controls shall be in line with technical standards.
 - Resilience shall be provided by design.

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

- Comprehensive protection entails protecting interconnections and other means of access to insider and outsider threats. When designing protection, the “human factor” shall be taken into consideration.
- Appropriate access controls on least privileges roles shall be part of application and access control design.
- **Detection**
 - For critical systems cyber security monitoring is essential, as performing security events monitoring and or analytics shall assist in detection and mitigation cyber incidents. These shall include third party providers also.
 - Please refer to ‘Security Policy: 2.14. Monitoring, Logging and Assessment.’
- **Response and Recovery**
 - It is not always possible to detect or prevent cyber incidents before they happen, even with the best processes in place. For this reason, incident response planning is of great importance. Resumption of services (if interrupted) shall be achieved within a reasonable timeframe, depending on the impact of the incidents and the criticality of the service. Contingency planning, design, and business integration as well as data integrity (also in the case of data sharing agreements) are key enablers for fast resumption.
 - For effective contingency planning, regular testing shall be conducted on regular intervals. Forensic readiness shall be facilitated for the investigations if needed.
 - Please refer to ‘Security Policy: 2.8. INCIDENT AND PROBLEM MANAGEMENT’
- **Testing**
 - Testing programmes, vulnerability assessments and penetration tests are cornerstones in the testing phase. Security testing shall be carried at different stages of application development and maintenance cycle. For detail please refer “Information Systems Acquisition and Development”, “Information Systems Maintenance”, “Network Security” and “Monitoring, Logging and Assessment” sections of “Information and Cyber Security Policy”.
- **Learning and Reporting**
 - RHFL shall continually re-evaluate the effectiveness of Cyber security management. Lessons learned from cyber events and cyber incidents contribute to improved planning. New developments in technology shall be monitored and include necessary actions into continual program.
 - Cyber security incidents which are critically affecting the business operations and large number of customers shall be reported to respective regulator and other governing bodies within the timelines defined by respective governing bodies.
 - RHFL shall report information security incidents, where the confidentiality, integrity, or availability of critical information is potentially compromised, to respective regulator and other governing bodies with the required data elements, as well as

any other available information, within timelines defined by respective governing bodies by Information Security Team, Security Operations Center (SOC), or information technology department. In some cases, it may not be feasible to have complete and validated information prior to reporting and RHFL shall provide their best estimate at the time of notification and report updated information as and when available.

- **Situational Awareness**

- Awareness contributes to the identification of cyber threats. Accordingly, the establishment of a threat intelligence process helps to mitigate cyber risk. In this regard, organizations shall participate in established information sharing initiatives.

2.17.3.3 Forensics

- **Prior to Analysis**


- RHFL employees must report system related incidents
- RHFL employees must not perform any action that may change the data held on the suspected device (being a device which is suspected of a security incident).
- Business/Unit shall handover the affected system to Information Security team.
- Information Security may take help of IT team depending on accessibility to impacted system.
- CITSO/IT Security Operations person shall store the device in a physically secured and access-controlled location to ensure data integrity is maintained until asset has been handed over to the external forensic expert.
- Information Security team shall engage forensic investigation team to carry investigations in concurrence with legal team.
- CISO/BISO shall ensure that external forensic experts are certified as well as competent for the job.
- CISO/BISO shall ensure that these external forensic experts are engaged by way of a formal engagement letter with a confidentiality clause. Non-disclosure agreement to be signed with the organization providing forensic services, before the experts are allowed further access.
- CITSO/IT Security Operations person shall ensure that document destruction is suspended immediately on impacted machine until further notice.
- CITSO/IT Security Operations person shall ensure that necessary information and rights are provided to CISO/BISO and forensic team.
- CITSO/IT Security Operations person shall ensure that necessary records are maintained for all the activities carried during forensic investigations.
- After forensic activity, CITSO/IT Security Operations person shall ensure that earlier access has been restored after approval from CISO/BISO/CRO.

- BISO shall ensure that the tools and methods used by external forensics experts are acceptable in the court of law. All forensic evidence shall be collected, stored and processed as per the applicable local laws and regulations.
- BISO shall ensure that chain of custody is maintained till closure of the forensic analysis and necessary records are maintained.
- **Examination**
 - External forensics expert shall perform bit-by-bit imaging of the data to have an exact copy for analysis. Forensic expert shall also perform a cryptographic checksum on original data to be able to validate data integrity in future.
 - External forensics expert shall extract the relevant pieces of information from the collected data.
- **Analysis**
 - External forensics expert shall perform the analysis of the relevant data and draw a time-line of the events.
 - External forensics expert shall use licensed tools only during the entire forensic activity.
- **Reporting**
 - External forensics expert shall prepare and provide a report detailing the root-cause. The report so generated shall solely be for benefit of RHFL and shall not be circulated to any third party without RHFL's express consent.
 - External forensics expert shall suggest appropriate recommendations for corrective and preventive actions in the report.
- **Protection of Evidence**
 - External forensics expert shall digitally sign the evidence gathered during the activity to ensure its integrity.
 - CISO/BISO/CRO shall ensure that forensic evidence so collected is encrypted for data security and handed over to relevant authorities.
 - Evidence gathered during the investigation shall be classified as confidential and secured as per Data Classification Policy.
 - Evidence shall be securely disposed after the expiry of its retention period in accordance with Asset Management Policy and Data Classification Policy unless it is required to be retained for an investigation/ regulatory compliance.

3 Glossary

Term	Description
RHFL	Reliance Home Finance Limited
ICSP	Information and Cyber Security Policy
IS	Information Security
ISRMC	Information Security Risk Management committee
RMC	Risk Management Committee
IT Act	Information Technology (IT) Act
NHB	National Housing Bank
IT	Information Technology
CRO	Chief Risk Officer
CTO	Chief Technology Officer
CITSO	Chief IT Security Officer
CISO	Chief Information Security Officer
CSO	Chief Security Officer
CPO	Chief People Officer
HR	Human Resources
CFO	Chief Finance Officer
COO	Chief Operating Officer
BISO	Business Information Security Officer
TRA	Technology Risk Assessments
BCP	Business Continuity Planning
DR	Disaster Recovery
RA	Risk Assessment
BIA	Business Impact Analysis
SOC	Security Operations Center
LAM	Logical Access Management
DLP	Data Leak Prevention
VA	Vulnerability Assessment
PT	Penetration Testing
VAPT	Vulnerability Assessment and Penetration Testing
SLA	Service Level Agreement
GRC	Governance Risk and Compliance

ERM	Enterprise Risk Management
IPR	Intellectual Property Rights
PII	personally identifiable information
SMS	Short Message Service
MAC	Media Access Control
CI	Configurations Item
IP address	Internet Protocol address
SPI	Sensitive Personal Information
OPI	Other Personal Information
IMEI	International Mobile Station Equipment Identity
AMC	Annual Maintenance Contracts
NDA	Non Disclosure Agreement
MBSS	Minimum Baseline Security Standards
OS	Operating System
CERT	Computer Emergency Response Team
OEM	Original Equipment Manufacturer
CR	Change Request
SAT	System Acceptance Testing
SIT	System Integration Testing
UAT	User Acceptance Testing
MPLS	Multiprotocol Label Switching
VM	Virtual Machine
VPN	Virtual Private Network
WiFi	Wireless Fidelity
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISDN cards	Integrated Services for Digital Network
CD	Compact Disk
DVD	Digital Video Disc or Digital Versatile Disc
ERT	Emergency Response Team
BMS	Building Management System
CCTV	Close circuit television

Document Title: Information And Cyber Security Policy	
Template Version: 5.3	
Last Updated: October 01, 2018	

4 Revision History

Version	Date	Description of changes	Approved by
1.0	27.01.07	<ul style="list-style-type: none"> Final version of the user policy 	Sandeep Phanasgaonkar
2.0	16.07.08	<ul style="list-style-type: none"> Revised version of user guidelines policy 	Sandeep Phanasgaonkar
3.0		<ul style="list-style-type: none"> Revised Policy 	Sandeep Phanasgaonkar
4.0	02.09.10	<ul style="list-style-type: none"> Modified – Physical, Handling confidential Information, Desktop/Laptop section, Added Blackberry 	Sandeep Phanasgaonkar
5.0	06.02.2014	<ul style="list-style-type: none"> Major change due to realignment of Information Security team with Enterprise Risk team. Organization structure as well as policies are changed for effective governance and security 	Lav Chaturvedi
5.1	21.1.2016	<ul style="list-style-type: none"> IS structure changes, User acceptable usage guidelines in detail, data classification of electronic records to align with IT Act 008 amendment, password policy reference in user access control, segregation of systems at network layer, key management policy enhancement 	Lav Chaturvedi
5.2	04.10.2017	<ul style="list-style-type: none"> Cloud Security Policy has been updated with new sections - Roles & Responsibilities, Compliance, Cloud vendor Offboarding, Legal terms, Virtualization controls and Cloud Service provider evaluation criteria before engagement and during engagement. Amendment made in line with the NHB Master Circular no. NHB (ND)/DRS/REG/MC-07/2017 dated July 1, 2017. 	Ravindra Sudhalkar
5.3	01.10.2018	<ul style="list-style-type: none"> Incorporated Cyber Security Policy into Information security Policy. Addition of ERT/CM (Crisis management) as new role and responsibility as per requirement of Cyber Security policy. New section of cyber security policy has been added to achieve cyber security resilience. 	Ravindra Sudhalkar