# Reliance Retail Finance Limited

## Information Security Policy

**Use and Interpretation of this document**



| | |
|---|---|
| Applicability | Reliance Retail Finance limited |
| Review Date | 09-04-2020 |
| Issuing Authority | Board of Directors |
| Content Owner | Board of Directors |

## Table of Contents

**Foreword**

This is the newly framed policy for Information Security, being released on behalf of IT department**.** The objective of this policy is to specify the minimum requirements for information security that the business shall follow

**Introduction**

The Reserve Bank of India has vide notification DNBS.PPD.No.04/66.15.001/2016-17 dated June 8, 2017 issued the Master Direction - Information Technology Framework for the NBFC Sector ("the IT Framework").

The Board of Directors of Reliance Retail Finance limited ("the Company" and / or "RRFL") at its meeting held on July 24, 2018 approved the Information Security Policy of the Company in accordance with the IT Framework. The Information Security Policy of the Company is effective from July 24, 2018.

Information Security Policy and Standards constitute sound business practice and shall assist RRFL in protecting information assets. This group policy represents the minimum requirements for information security that the business shall follow. In addition, business may be required to incorporate additional information security practices and procedures as part of their compliance with other policies.

RRFL under the direction of it's the Information Technology Strategy Committee has documented the Information Security Requirements.

## 1. Scope and Exclusions

The Information Security Policy applies to RRFL and its affiliates, subsidiaries, personnel, third party consultants, contractors, vendors and any individual or entity that is provided access to the RRFL information assets. The scope also includes all information assets belonging to RRFL.

## 2. Required References

Group Information Security Policy

## 3. Symbols and Abbreviations

The terms in use in the document are explained below:

RRFL: Reliance Retail Finance limited

CIO: Chief Information Officer

## 4. Reliance Retail Finance limited Requirements

### 4.1. Management Commitment

4.1.1. Top management shall demonstrate leadership and commitment with respect to the information security management system by:

- Ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization.
- Ensuring the integration of the information security management system requirements into the organization's processes;
- Ensuring that the resources needed for the information security management system are available.
- Communicating the importance of effective information security management and of conforming to the information security management system requirements.
- Promoting continual improvement.

### 4.2. Segregation of functions

4.2.1. There should be segregation of the duties of the Information Security Team and Information Technology division.

4.2.2. The Information security function should be adequately resourced in terms of the number of staff, level of skill and tools or techniques like risk assessment, security architecture, vulnerability assessment, forensic assessment, etc.

4.2.3. There should be a clear segregation of responsibilities relating to system administration, database administration and transaction processing.

### 4.3. Information Risk Management

Information risks shall be continuously identified, assessed and evaluated. Mitigation measures shall be evaluated based on the business impact of the risk and with regard to efficiency, cost and practical feasibility.

4.3.1. Risk Assessment

4.3.1.1. CIO shall designate Information Owners for RRFL Information under their control.

4.3.1.2. All Information assets belonging to RRFL shall be assessed periodically by the Information Asset Owner based on the defined Information Risk Management Framework and appropriate controls implemented and monitored regularly for effectiveness and efficiency.

### 4.4. Human Resource Security

Security requirements shall be integrated with HR processes at all stages of employee/ third-party personnel association with RRFL including during recruitment/ selection, employment/ engagement and termination/cessation.

4.4.1. Prior Employment:

4.4.1.1. Security roles and responsibilities for employees and contractors shall be clarified and understood and a confidentiality agreement shall be signed by employees and contractors and other who may gain access to RRFL confidential, proprietary and/or internal information.

4.4.1.2. Proper Background check and screening shall be conducted for resources hired for business critical or any privileged roles.

4.4.2. During Employment:

4.4.2.1. Information Security Team shall ensure that the Information Security Policy is communicated to all the employees/contractors and all who have access to RRFL Information Systems.

4.4.2.2. All employees and contractors shall receive adequate and on-going training regarding the Information security policy and relevant standards and guidelines.

4.4.3. Termination or change of Employment Responsibility

4.4.3.1. All physical and logical access privileges shall be revoked immediately when a user no longer requires access to information or systems as part of their job, or when they leave RRFL.

4.4.3.2. Upon termination of employment, contract or agreement internal staff and third party personnel shall:

- Return assets that belong to RRFL; and
- Confirm (in writing) that they have destroyed all copies of information owned by RRFL.

## 4.5. **Asset Management**

4.5.1. All information assets of RRFL shall be clearly identified and inventory of all such assets shall be drawn up and maintained by designated Information Asset Owner(s).

4.5.2. Appropriate Security protection shall be provided throughout the lifecycle as per the criticality and sensitivity level of the information assets.

## 4.6. **Information Classification**

4.6.1. Information Classification levels shall be defined as per confidentiality requirements.

4.6.2. Information Owners shall ensure that all the RRFL Information under their control are classified into one of the defined levels.

## 4.7. **Access Control**

4.7.1. Business shall ensure that all the technology platforms will authenticate the identity of users (including other systems accessing these platforms) prior to initiating a session.

4.7.2. All users shall be identified to the technology platform by:

4.7.2.1. Unique User ID.

4.7.2.2. Method of authentication enabling unique identification of the user e.g., a static or dynamic password, public key, biometric or other authentication mechanism.

4.7.3. Users shall be held accountable for all activity associated with their User ID and password.

4.7.4. All the authorization shall be based on the need-to-know basis and will be reviewed periodically.

4.7.5. Each User Role shall be defined and documented. Delegation of authority for right to upgrade or change user profiles and permissions and also key business parameters shall be documented.

4.7.6. Business shall ensure there is at least 2 level of authorization for completion of financial transaction in information system.

4.8. **Cryptography**

4.8.1. Business shall ensure that all Information Systems use only approved Cryptographic algorithms, key lengths, key management and Security protocols.

4.9. **Physical and Environmental Security**

4.9.1. All RRFL facilities and information assets shall have appropriate physical access controls in place to protect them from unauthorized physical access and shall be safeguarded against environmental hazards.

4.10. **Operations Security**

4.10.1. Business in co-ordination with Information Security Team shall plan, design, implement the security requirement for endpoints, servers and networks and monitor them an on-going basis.

4.10.2. The Security requirement shall inter alia include Change Management, Segregation of duties. Vulnerability Management, Threat Management, Control against malware, Information back up, Logging and monitoring, Security Analytics and Assurance.

4.10.3. All audit trails shall be stored for all IT assets to comply with legal, regulatory and contractual requirements

4.11. **Patch Management**

4.11.1. A formal patch management process shall be established and documented to identify, review, test and implement patches to information systems in a timely manner.

4.11.2. Patches that are determined as critical shall be installed within 48 hours of release.

4.12. **Communications Security**

4.12.1. All RRFL network communications shall be ensured and protected with appropriate level of security controls to protect information in systems and

applications. Public Key Infrastructure can be used to ensure confidentiality of data, access control, data integrity, authentication and nonrepudiation wherever necessary.

4.12.2. Communications Security controls shall include, but is not limited to, segregation of networks, service levels and management controls based on the Risk Assessment results.

4.12.3. Exchange of information within RRFL and between RRFL and external entities for business purpose shall be protected against unauthorized disclosure and inappropriate modification by implementing adequate security controls.

### 4.13. System Acquisition, Development and Maintenance

4.13.1. Appropriate security controls shall be implemented to ensure that acquisition, developments and maintenance of information do not have negative impact regarding confidentiality, integrity, availability and authenticity of RRFL information assets.

4.13.2. Duties and responsibilities shall be separated in a manner reducing the possibility of unauthorized or unforeseen abuse of RRFL information assets.

### 4.14. Supplier Relationships

A risk assessment of RRFL information systems service providers shall be performed and the vendors shall be classified by risk profile. Access to information assets granted to suppliers shall be regularly monitored and reviewed and any change shall be done through controlled process.

### 4.15. Information Security Incident Management

4.15.1. A process to identify, report, classify, respond, escalate and recover from information security events in a timely manner shall be established and maintained.

4.15.2. All employees, contractors and third party users should be made aware of the process of reporting the different type of information security events having an impact on security of RRFL's information assets.

### 4.16. Information Security Aspects of Business Continuity Management

4.16.1. Business shall determine its requirement for information security and the continuity of Information Security Management in adverse situations e.g. during a crisis or disaster.

4.16.2. Business in co-ordination with Information Security shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for Information security during an adverse situation.

4.16.3. Business in co-ordination with Information Security Team shall verify the established and implemented information security continuity controls at

regular intervals in order to ensure that they are valid and effective during adverse situations.

### 4.17. Privacy

4.17.1. Business shall ensure, at all times, the privacy of and endeavor to keep safe any and all personal data collected and/or stored and/or transmitted and/or used for, or on behalf of RRFL.

4.17.2. Business shall endeavor to ensure all collection, storage, transmission and other handling or usage of personal data by the organization shall be done in accordance with this policy and applicable Legal & Regulatory requirements.

### 4.18. Compliance

4.18.1. Business shall ensure that its employees and external providers comply with the applicable sections of the RRFL Information Security Policy and its associated standards as well as applicable Legal, Contractual and Regulatory requirements.

4.18.2. CIO shall ensure compliance with the Information Security Policy appropriate to the level of acceptable risk.

4.18.3. The Internal Control & Audit department shall audit operational integrity for compliance with the RRFL Information Security Policy. Deviations, if any, shall be reported for management action.

### 4.19. Deviations

4.19.1. There may be genuine business reasons for exceptions. Any exceptions to this policy should be raised by the business through the respective CIO. All exceptions to security policy will be approved by the Information Technology Strategy Committee.

4.19.2. Information Security Team shall ensure that appropriate compensatory controls are in place before recommending the exception.

### 4.20. Consequence management & Non-compliance

4.20.1. All violations of security policies, standards and/or guidelines are subject to disciplinary action. The specific disciplinary action depends upon the nature of the violation, the impact of the violation on informational assets and related facilities, etc. Violations will be handled as per the existing HR processes and could range from a verbal reprimand, to termination of employment/contract and/or legal action.

## Annexure

N/A

## Supporting Reference

N/A

## Version Control

| Versions | Release Date | Summary of changes |
|---|---|---|
| 1.0 | TBU | Initial Document Creation |
| 2.0 | 09-04-2020 | Realigned as per regulatory requirement and Industry best practices. |