Information Technology Policy

Table of Contents

Document Control

Version History:

Date	Version	Description of change	Owner	Approved by
27-Dec-17	V1.0	RHF IT Policy document	RHFL	Shashi Ravulapaty
10-Oct-18	V1.1	RHF IT Policy document Annual Review, Consolidation of 19 Policies to 1 Policy	RHFL	Kunal Dikshit
27-SEPT-19	V1.2	RHF IT Policy document Annual Review, Anti-malware Policy	RHFL	Kunal Dikshit

Authorization:

Prepared By	Reviewed By	Approved By
Name: Chaitanya Sukum Date: 27-SEPT-19	Name: Lalit Kumar Rout Signature: Designation: Head IT & Security Date: 30-SEPT-19	Name: Kunal Dikshit Signature: Designation: CTO Date: 30-SEPT-19

Distribution List:

Sr. No	Department or Function Name
1	BOD
2	Strategy Committee
3	Steering Committee
4	Process Owners/Functional Head
5	Users

A. Purpose

This policy defines the requirements to protect the IT infrastructure of Reliance Home Finance Limited.

The purpose of this policy is to provide guidelines to all who use and manage Information Technology (IT) resources and services (including but not limited to computing, networking, communications and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, and any related materials and services)

B. Scope and Applicability

1.1 Reliance Home Finance Limited. Reliance Centre, South Wing, 6th Floor, Off Western Express Highway, Santacruz East, Mumbai – 400055 and branches.

1.2 All employees, consultants and vendors.

C. IT Policy

1 Anti-Malware

1.1 Policy

1.1.1 Anti Malware Management Policy shall be implemented and constantly monitored for ensuring adequate protection and prevention of IT resources against computer viruses and other virus like/mobile code infection activities at various operating levels.

1.1.2 IT team shall be responsible for keeping their systems running with antivirus software which is updated with latest antivirus update.

1.1.3 Systems shall be restricted through hardening process for the desktop/laptop environment. The hardening process shall be uniformly deployed across the entire organization.

1.1.4 Critical Systems at third party end shall also follow the same Malicious Code and Mobile Code security when their systems are used for RHFL's related activities or accessing RHFL network.

1.1.5 Review of virus definitions updates shall be done by the IT team on a predefined basis. IT team, through a formal process, shall ensure that all systems have been updated with the most current OS patches to address known vulnerabilities.

1.1.6 Employees shall not be permitted to install any tool/application/freeware on RHFL systems without approval from the IT team.

1.1.7 Roles and responsibilities of the IT team responsible for protection of the company's systems against mobile code and malicious code shall be defined and adhered to.

1.1.8 Process(es) shall be implemented to proactively monitoring and/or to receive and/to review new malicious or mobile code technical information from the antivirus vendor

1.1.9 At any given time, RHFL shall demonstrate protection from malicious/mobile code for the entire computing environment.

1.1.10 Systems where RHFL's information is processed shall follow same Anti Malware Management Policy and Procedure across all locations.

1.1.11 Virus definitions/OS patches shall be updated on a predefined time period (when the system gets connected to the network) on all systems.

1.1.12 Users shall not be allowed to download /possess /run unauthorized software /freeware/ tools.

1.1.13 Proactive monitoring /reviewing technical information of malicious codes shall be implemented to mitigate associated risks.

1.1.14 Monitoring of desktops/laptops shall be done to ascertain gaps in implementation on a monthly basis.

1.1.15 All identified vulnerable & critical systems shall always be protected on priority basis.

1.1.16 Malicious code or mobile code definitions which are not addressed by the existing tools shall be reported and resolved within two working day of getting infected.

2 Asset Management

2.1 Policy

2.1.1 RHFL shall identify and document all IT assets under critical processes

2.1.2 All IT assets shall have identified owners who will be responsible for the asset

2.1.3 Asset inventory shall be reviewed and updated at least once annually

2.1.4 Owners of assets shall classify all their IT assets

2.1.5 RHFL shall define an information classification scheme and guidelines to classify and handle IT assets

2.1.6 RHFL shall label all physical assets with appropriate tags

2.1.7 RHFL shall procure all IT equipment through a standardized process. The IT department and the finance department shall be responsible for this process.

3 Backup and Restoration

3.1 Policy

3.1.1 Backup of all business data, related application systems and other business critical applications shall be done as per the master backup plan along with frequency agreed with the data owners.

3.1.2 Back up options shall be considered depending on the availability needs of the data owner and the recovery options during a disaster or loss of data due to errors and omissions either advertent or inadvertent.

3.1.3 Corporate information/ records/ data are all paper or electronic form that are produced by you as an employee including but not limited to memoranda, email, contracts, future plans, designs etc. are important.

3.1.4 All the information/ records/ data shall be archived for 20 years. Archiving shall be done to ensure that stakeholders have easy access on a need to know basis of the data / information.

3.1.5 Data backup strategy and data recovery procedures shall be implemented to ensure that critical business data is never lost under any circumstances and is always available.

3.1.6 Adequate backup space for the identified users/department shall be provided to backup locally stored data.

3.1.7 If any external parties are to be involved for data back up or recovery, then adequate care shall be taken to protect the information assets of RHFL's given to these agencies.

3.1.8 Media handling for backup / restoration activities during normal business operation and that during a DR shall be done in a secure manner.

3.1.9 Adequate security shall be provided to the area (onsite and offsite) which shall house back up media and sitting norms shall be adhered to.

4 BYOD (Bring Your Own Device)

4.1 Policy

4.1.1 Provisioning of mobile computing devices such as smart phones, tablets with phone capability, tablets without phone capability but with Wi-Fi and data access capabilities shall be done based on demonstrated business need by MDM manager and BISO and/or HOD (DEPARTMENT HEAD) as the case may be. Currently BYOD (Bring Your Own Device) policy has not been extended to personal laptops. This shall form a part of the evolving and future business needs.

4.1.2 There shall be formal process for provisioning/de- provisioning of mobile devices for use in corporate environment.

4.1.3 MDM tool is deployed for mail access through employee's mobile devices.

4.1.4 Adequate and enough levels of physical and logical security controls shall be deployed on these mobile devices.

4.1.5 Appropriate technology platforms shall be promulgated to ensure management of mobile devices with diverse operating systems in a seamless manner with required security controls.

4.1.6 Availability of RHFL network delivered services shall be of critical importance to the users who use such computing devices and the technical support shall support this criticality.

4.1.7 Acceptable usage norms shall be articulated to the user.

4.1.8 RHFL shall prescribe permissible applications and services that can be mounted on such device to access corporate data.

5 Capacity Management

5.1 Policy

5.1.1 Capacity Planning is required to be undertaken by IT to facilitate in the meeting of operational and business objective of the company in order to address the current and future needs in a structured, formal approach.

5.1.2 Capacity planning shall also encompass information technology personnel who are directly responsible for the maintenance and functioning of the enterprise wide information systems infrastructure.

5.1.3 It is desired that all the IT resources usage are monitored in terms of average usage in a standardized manner and if any deficiency found then that shall be reported to identified group as the case may be for remedial action.

5.1.4 Capacity planning shall be initiated for IT resources and services, keeping in mind the present and future requirements are in consonance with the long-term business vision and growth.

5.1.5 RHFL shall adopt a formal process for assessment of capacity utilization periodically and that of planning on a yearly basis.

5.1.6 Periodic reviews shall be planned.

6 Cryptography

6.1 Policy

6.1.1 Data Encryption

#	Policy Summary	Policy Description
1.	Management shall decide on use of cryptography	To prevent loss, theft or unauthorized disclosure of certain information which could be detrimental to RHFL, the management shall decide to apply cryptographic techniques depending on the information.
2.	Appropriate encryption shall be used for remote access	Whenever possible and appropriate, encryption shall be used to support security of remote access connections to the RHFL's network and computing resources.
3.	Web service shall be HTTPS enabled where possible	Depending on the business requirement, RHFL web services that involve the transfer of sensitive or confidential data shall use encryption for e.g. HTTPS.
4.	Encrypted backup shall be securely stored	Where it is not practical to encrypt backup, it shall be stored securely with appropriate physical security measures.
5.	RHFL shall have right to view user encrypted data	RHFL shall reserve the rights to request sight, at any time, of unencrypted version of data stored on its system by users using their own encryption. It also shall have right to remove such data.
6.	Standard encryption technique shall be used	All encryption products, standards used to protect RHFL sensitive data shall be ones that have received substantial public review and have been proven to work effectively.

6.1.2 Cryptographic Key Management

#	Policy Summary	Policy Description
7.	Encryption key shall be securely stored	Encryption keys shall be stored and communicated securely.
8.	Encryption key shall be managed based on standard practice	Encryption keys shall be managed in a way that ensures encrypted stored data will neither become unrecoverable nor accessible by an unauthorized person.
9.	Encryption key shall be easily accessible during emergency	The encryption key shall be managed to facilitate authorized user to obtain prompt access to the encrypted information in the case of emergency or investigation.
10.	Encryption key shall be revoked when not needed	Encryption key shall be revoked when the holders leaves the organization.

7 E-mail Management

7.1 Policy

7.1.1 E-mail facility will be provided to all employees.

7.1.2 E-mail Management Policy outlines the guidance and responsibilities to ensure that RHFL E-mail system is not misused and serves as an efficient mode of business communication.

7.1.3 The E-mail system of RHFL given to employees is an asset of RHFL and can be subject to periodic audits to monitor compliance to business objective and values.

7.1.4 RHFL shall ensure that E-mail service and operations remain secure and efficient while communicating internally as well with external parties.

7.1.5 Users shall use company provided E-mail infrastructure for official purposes only and not for personal communication.

7.1.6 Usage of personal E-mails like G-MAIL, YAHOO MAIL, HOTMAIL or any other E-mail system is prohibited using RHFL infrastructure.

7.1.7 All users of E-mail facility will be provided with a unique E-mail ID.

7.1.8 RHFL IT department reserves the right to monitor (at any time or as the need may be, or upon the request of a reporting manager) contents transmitted by users using RHFL's E-mail systems.

7.1.9 E-mail facility will be owned by an individual. Shared ownership of email facility is not permitted.

7.1.10 E-mail administration shall be the responsibility of RHFL's IT Team.

7.1.11 All incoming E-mails will be scanned for viruses.

8 End Point System Security

8.1 Policy

8.1.1 Formal security maintenance process shall be implemented to ensure adequate security at the end user computing system level. Access to end point computing systems shall be restricted to those people who need the information to perform their business functions on a strictly need to know basis. System documentation shall be protected against unauthorized access. The reference to the word “system(s)” hereafter in this document shall be construed as end point computing systems like desktops, laptops, smart phones & tablets. Wherever required to be stated separately, the same shall be done to elicit a particular detail. However, the security management of smartphones, tablets and blackberry devices has been articulated in the BYOD Policy.

8.1.2 IT team shall be responsible to ensure that systems are updated and functional with current operating system patches and antivirus updates. Systems shall be hardened, and appropriate maintenance activity shall be carried out for the system(s) to work optimally.

8.1.3 Use of system utilities which may override system or application control shall be done only under authorization.

8.1.4 Each user shall be provided a unique user ID and password. Password management shall be done to ensure that quality and complexity of passwords is maintained. A formal user registration and de-registration process shall be established. Password complexity shall be as defined in the Password Policy and Procedure.

8.1.5 For critical systems, session time out and connection time out shall be enforced wherever possible. If required, login procedures for these systems shall be secure and shall comprise of multifactor factor authentication techniques.

8.1.6 Systems shall be configured such that users shall be able to lock their terminals either manually or automatically to prevent unauthorized access.

8.1.7 Any changes done to systems shall be through a formal change management process.

8.1.8 When any changes are done to the operating systems, the new system shall be tested before deployment to the assigned personnel.

8.1.9 Suitable tools shall be deployed to manage integrated roll out of OS patches and AV updates and initiate remediation measures to remove inconsistencies in deployment.

9 Incident Service Desk Management

9.1 Policy

9.1.1 In order to understand as to how this policy shall manifest, it is imperative that one understands the meaning of what an Incident or Event is. The explanation is provided as under:

9.1.1.1 An event is defined as an identified occurrence in a system, service or network indicating a possible breach of security, procedures and safeguards a previously unknown situation that shall be relevant from the security point of view.

9.1.1.2 An incident is defined as a single or a series of unwanted or unexpected events that have a significant probability of compromising business operations and threatening security.

9.1.1.3 A crisis shall manifest out of an incident, if it threatens the safety of the staff, and impacts business continuity. Anything else shall be construed/deemed as incidents/events.

9.1.1.4 Note: For the sake of brevity, this document shall only address incident service desk management policy whereas aspects of crisis (es) shall be dealt with in Business Continuity Planning / Management and Crisis Management Documents.

9.1.2 RHFL shall develop, communicate and implement formal systems and procedures for detecting and reporting incidents. It shall be ensured that the incidents and weaknesses are reported in time to the appropriate authorities and corrective actions are taken immediately to contain the damage and avoid the recurrence of such events in future.

9.1.3 Appropriate tools shall be provided to employees. RHFL shall endeavor to integrate existing platforms like helpdesk ticketing tool, with a unified Incident Service Desk Management Portal.

9.1.4 RHFL shall ensure that all the risks related to incident reporting and possible controls to address those risks are identified and mitigated.

9.1.5 Necessary Incident Service Desk Management Maps along with Standard Response procedures shall be developed by the respective teams. So also aspects of problem management shall also be addressed. Corrective and Preventive action shall be applied as an outcome of the problem management process so as to minimize the occurrence of the incident.

9.1.6 Incident register shall be maintained, reviewed and updated on a yearly basis

9.1.7 RHFL shall establish a formal disciplinary process for dealing with employees who commit security breaches.

9.1.8 Individual teams shall develop related to incident service desk management, problem management and update their knowledge in a formal manner.

9.1.8.1 Employees shall be trained on the incident service desk management process from the perspective of individual action.

9.1.8.2 The incidents shall be categorized in levels to reflect potential business impact. Based on the nature of the incidents, RHFL shall at all times ensure that the relevant applicable legislations (IT Act 2008 amendment) are adhered to, evidences related to the incidents are protected and aspects of cross border law if any are addressed adequately.

9.1.8.3 The management shall share learning's from incident service desk management through awareness programs and also encourage employees to report incidents.

9.1.8.4 The management shall also address security weaknesses in technology, information systems, as part of Incident Service Desk Management and create action plans to prevent and control re-occurrence of incidents in these areas.

10 Internet Usage

10.1 Policy

10.1.1 RHFL encourages the use of internet to expedite their business work process. But internet connectivity presents the company with new risks that needs to be addressed in order to safeguard vital information assets.

10.1.2 Internet facility shall be provided to employees on a need based basis through a formal process of approval.

10.1.3 There shall be a defined mechanism to monitor, block and check the content which has been accessed by employees via the internet from within the RHFL network or from their mobile devices, laptops, phones when outside the RHFL network.

10.1.4 Employees using internet on company's assets shall always ensure that usage shall not compromise or expose the network and / or assets of RHFL to external threats.

10.1.5 RHFL reserves the right to revoke or suspend internet use, should a business situation warrant such a step.

11 Logical Access Control

11.1 Policy

11.1.1 All logical access paths to the information of RHFL shall be controlled to prevent, detect, and minimize the effects of unintended or unauthorized access and information leakage.

11.1.2 Access control shall be established by imposing standards for protection at the Operating System level, at the Application level and at the Database level. Access to RHFL computer systems shall be based on the principles of least privilege and "need to know" principle and must be administered to ensure that the appropriate level of access control is applied to users as well as system support personnel to protect the information of RHFL.

11.1.3 The level of control imposed should reflect the nature and importance of the information to be protected.

11.1.4 There shall be a formal registration and de-registration process established in providing access to information systems for employees and third parties of RHFL.

11.1.5 IT team shall periodically review the access rights provided through a formal process.

11.1.6 Access to the identified critical information systems (Services / Applications / Servers / Devices etc.) of RHFL shall happen through a secure log-on process. Access shall be provided on a strictly need to know basis.

11.1.7 Access to RHFL's network for third parties is provided in a restricted way.

11.1.8 All connections to RHFL resources from outside the RHFL office must adhere to the RHFL's Information Technology Policy.

11.1.9 All equipment used for remote access to connect to RHFL's information resources must meet RHFL remote access requirements.

11.1.10 All logical access shall be revoked upon exit/ termination of employment of RHFL Users. IT team may revoke privileged access to sensitive information or information processing assets during the notice period itself, if advised by the HOD.

12 Mobile Computing and Teleworking

12.1 Policy

12.1.1 A secure access control mechanism shall be provided when connecting to RHFL network and shall necessarily have one factor authentication mechanisms.

12.1.2 Users shall ensure that their computing devices are maintained in a secure manner and the threats of loss or theft of the device are adequately addressed.

12.1.3 IT Team shall be responsible for the security of information held on such devices.

12.1.4 An authorization process shall be established for provision of mobile computing and teleworking services, based on roles and responsibilities. Regular review and monitoring shall be done by the IT Team.

12.1.5 Protection from malicious code, application of encryption shall be applicable on mobile devices used in teleworking and mobile computing.

12.1.6 Procurement of devices required for mobile computing and teleworking shall be through official channels only and shall abide by the security requirements of RHFL.

12.1.7 Cryptographic controls shall be used wherever necessary as a means of data protection.

12.1.8 Personal laptops/PDAs/ Tablets shall not be permissible for official usage.

13 Network Security

13.1 Policy

13.1.1 The Network Infrastructure of RHFL shall be managed and controlled so as to prevent internal and external threats to its information systems, applications and services. Adequate protection shall be provided for the same.

13.1.2 This objective shall be achieved through the establishment of security controls like: management of system documentation, access control to identified network devices, services and applications, establishment of service level agreements with third party service providers for all outsourced services, equipment siting and protection, incident management and change control.

13.1.3 Network shall be adequately protected from any possible threats emanating from Mobile Computing, Teleworking, On–Line transactions and internal traffic between users on the premises.

13.1.4 Controls to prevent incomplete transactions, misrouting, unauthorized message alteration, duplication, abetment of fraudulent activity and information leakage shall be implemented.

13.1.5 The physical and logical access to diagnostic and configuration ports shall be restricted.

13.1.6 Employees and/or third parties using the network services of RHFL shall be provided with access rights on a need to know basis through a formal process.

13.1.7 Monitoring of the identified network parameters shall be done by the IT team.

13.1.8 Secure log management process shall be established wherein logs getting generated at user, administrator level are captured. System related log information shall be captured for further analysis and necessary action.

13.1.9 For the logged information to be consistent and meaningful, all the servers and networking devices shall have their system clocks synchronized either manually by the system administrator or an automated process using a NTP server or through AD as reference.

13.1.10 Formal mechanism for recording and redress of faults, events and incidents shall be deployed by the System Administrator.

13.1.11 The roles and responsibilities for management of network security shall be clearly defined, communicated and reviewed on a regular basis to ensure optimum operative effectiveness and necessary segregation of duties shall be done to attain the said objective.

13.1.12 Changes done to the network devices comprising of settings or configuration settings shall be done through the existing process of change control in RHFL by the IT team.

13.1.13 A formal process for managing the inventory of devices and applications being deployed for network administration and management shall be in line with the organizations framework.

14 Password Management

14.1 Policy

14.1.1 All RHFL information technology resources should have appropriate password controls in place to protect IT / Information assets from unauthorized access.

14.1.2 Password controls should include managing password complexity, periodicity (change interval) and length which should be enforceable by the system.

14.1.3 A formal process for password management shall be implemented for employees and concerned third parties.

14.1.4 Employees should be provided with training on creation and use of strong passwords.

14.1.5 Passwords should not be shared without due authorization.

14.1.6 Default passwords, provided by the vendor for systems, network devices, applications should be changed on first instance of usage or as per hardening procedure.

14.1.7 Default user IDs (provided in the application package, network devices, operating systems, databases etc.) shall be disabled before moving into production.

14.1.8 Users shall be provided with individual logon IDs for tracing accountability.

14.1.9 Generic logon IDs shall not be used by individuals unless needed for genuine business needs, such exceptions shall be documented.

14.1.10 Privileged ID (super user) and password should be set and managed for servers, network devices and applications.

14.1.11 All servers and network devices should have double-factor authentications wherever possible.

15 Patch Management

15.1 Policy

15.1.1 IT Infrastructure (Workstation & Server Operating Systems, Applications, Databases, Storage & Network devices etc.) shall be patched in accordance with the patching procedure.

15.1.2 Any system version upgrades/patch deployments shall be done considering compatibility to RHFL environment. A through impact analysis shall be done considering version/patch stability, possible issues etc.

15.1.3 Business and technical impact of implementing, or not implementing, a particular patch shall be assessed. Patches will be tested on test environment prior to production deployment

15.1.4 Operating Systems, Applications, Databases, Networking Devices and Storage devices shall be deployed with OEM's latest version provided it offers stability to RHFL IT environment. Any exceptions with version/patch upgrades will be documented.

15.1.5 An exception process shall be implemented in the event that a patch cannot be deployed or if no patch is available for an identified vulnerability. This process must include a risk assessment and proposed mitigating controls.

16 Application Management

16.1 Policy

16.1.1 Required level of security shall exist to ensure the availability, integrity and confidentiality of all applications and the associated data. It shall be ensured that access to the applications is authorized and on a need to know basis, changes made to these are adequately controlled and audit trails are provided to log and detect any unauthorized activities.

16.1.2 Security requirements for application development or modification to existing applications at RHFL are defined, agreed and documented as part of the overall business case for the system.

16.1.3 Acquisition, development and deployment of software applications that are used in RHFL addresses confidentiality, integrity and availability of the information.

16.1.4 Appropriate security is maintained in the development and support processes by controlling the development, live and support/test environment. Software code shall be in a library with access to authorized personnel with a check-in and check-out process.

16.1.5 Checks shall be applied for ensuring data input is validated and correctness is maintained. Similarly checks for validation of data output shall be present. Also session inactivity time-outs and connection time outs shall be implemented to prevent unauthorized access.

16.1.6 Its integrity compromised for want of validation checks during input and output either through processing errors or through motivated personnel.

16.1.7 The RHFL shall implement controls to ensure that data integrity, confidentiality and availability are maintained in all applications including those in Electronic Commerce / Online transaction applications.

16.1.8 All outsourced software development shall be under RHFL's control and shall be monitored and supervised.

16.1.9 Formal process shall be instituted for making changes to the packaged software after obtaining consent from the software vendor and also after careful analysis of the business requirement and possible impact on the existing environment after modifications are live.

16.1.10 The test and production environment shall be separate along with separate VLAN for each of them.

16.1.11 Process shall be implemented to monitor, review and address the known technical vulnerabilities in applications by either taking support for external agencies or performing the same through the identified group/ISG within the RHFL.

16.1.12 Any software copyright violation by employees shall lead to a disciplinary action even leading to a legal action as the case may be.

16.1.13 RHFL information technology infrastructure and applications shall only be licensed softwares deployed on them for the development of internal applications.

16.1.14 Suitable technology solution shall be deployed which shall manage application monitoring to facilitate in better management of resources and also track incidents arising out of application use.

17 Application Change Management

17.1 Policy

17.1.1 Department Application Spoc will initiate a change request with approval of Department HOD.

17.1.2 RHFL shall employ a formal mechanism to capture change requests emerging from the business groups and the technology groups.

17.1.3 All application changes before getting executed shall be formally approved by a concerned stakeholders from business and technology groups.

17.1.4 Application Change Requests shall be dealt with, in terms of their importance and impact on the business.

17.1.5 All application change requests made and closed in the affirmative or those which have been denied / delayed or escalated shall be documented in a pre-prescribed format and detail. Records of the change requests shall be maintained by the process owner for audit purposes.

17.1.6 No changes to the information systems shall be made without valid and authorized change control approval in place.

17.1.7 A formal review of all changes done to RHFL's information systems and infrastructure shall be conducted.

18 Infra Change Management

18.1 Policy

18.1.1 Application owner/ IT Manager will initiate a change request.

18.1.2 RHFL shall employ a formal mechanism to capture change requests emerging from the business groups and the technology groups.

18.1.3 All infra changes before getting executed shall be formally approved by a concerned stakeholders from business and technology groups.

18.1.4 Infra Change Requests shall be dealt with, in terms of their importance and impact on the business.

18.1.5 All infra change requests made and closed in the affirmative or those which have been denied / delayed or escalated shall be documented in a pre-prescribed format and detail. Records of the change requests shall be maintained by the process owner for audit purposes.

18.1.6 No changes to the information systems shall be made without valid and authorized change control approval in place.

18.1.7 A formal review of all changes done to RHFL's information systems and infrastructure shall be conducted.

19 IT Governance Training

19.1 Policy

19.1.1 If required, all employees, consultants and vendors shall be imparted appropriate information technology training. They shall be regularly updated with the organizational information technology policies and procedures relevant for their job function.

19.1.2 Information Technology training shall be imparted at the time of induction to all new employees and in case of existing employees it will be ensured that they undergo this training at the earliest. All RHFL employees shall undergo refresher trainings, on periodic basis, which shall be at least once in a year.

19.1.3 The training content shall be updated taking into consideration the IT incidents, the changes in the business, contractual, legal or regulatory requirements. CISO (Chief Information Security Manager) is responsible for updation and creation of the training content.

19.1.4 Evaluation of the awareness of the employees will be done on a periodic basis through surveys / training sessions conducted online or offline by HR/respective department.

D. Enforcement

1.1 Any employee found to have violated this policy shall be subjected to disciplinary action as per the RHFL's Code of Conduct.
1.2 Management's interpretation of the clauses in this policy will be final and binding. Management reserves the rights to alter or amend any clause in this policy at any time as per its discretion.
1.3 Exceptions and deviations to this policy shall be documented and approved by BISO/CTO/CISO. The business need for the same shall be detailed.
1.4 Any instruction from IT team needs to be adhered by the users.

E. Exception

1.5 Exceptions shall not be universal but shall be granted by the IT Strategy Committee on a case-by-case basis, upon official request made by the information owner. All Exceptions granted by the IT Strategy Committee must have a definite end date. These may arise, for example, because of local circumstances, conditions or legal reason existing at any point of time.
1.6 Exceptions to the IT Training Policy may have to be allowed at the time of implementation of this policy or at the time of making any updation to this document or after implementation on an ad-hoc basis based on business or a specific and a peculiar manifestation of circumstances which could be of temporary or permanent in nature.
1.7 All exceptions during implementation shall be submitted by the concerned person responsible for implementation. These shall be submitted through an Exception Form (Prakriya Portal) and sign-off on the same shall be maintained including ad-hoc requests.
1.8 The BISO/CTO/CISO shall review all exceptions, as the case may be, every six months for validity and continuity.

F. Violation and Disciplinary Action

1.9 RHFL shall at all times protect the interests of its stakeholders through the adherence to Anti-Malware, Asset Management, Backup and restoration, Bring your own device(BYOD), Capacity Management, E-mail Management, End Point System Management, Incident Service Desk Management, Logical Access Procedure Network Management, Password Management, Patch Management, Application Management, Application Change Management, Infra Change Management IT Governance Training Policy and applicable legislation and through the administrative mechanism established coupled with the Policy, RHFL's shall control the occurrence of violations by individuals.
1.10 Violations by the third parties shall also come under the purview of this policy and action shall be taken accordingly.

G. Disclaimer

1.11 RHFL reserves all rights and is the exclusive owner of all intellectual property rights over this Anti-Malware, Asset Management, Backup and restoration, Bring your own device(BYOD), Capacity Management, E-mail Management, End Point System Management, Incident Service Desk Management, Logical Access Procedure Network Management, Password

Management, Patch Management, Application Management, Application Change Management, Infra Change Management IT Governance Training Policy document. This document shall not, either in part or in full, be reproduced, published, copied, displayed, distributed, transferred, stored into any media (such as hard disks, USB Drives, Pen Drives, Memory Cards, CDS, DVD's), and/or captured or transmitted through by any means (electronic, digital, mechanical, photocopying, recordings, video and film or photographs and otherwise) by any person without prior written consent from the IT Governance team of RHFL. Anti-Malware, Asset Management, Backup and restoration, Bring your own device(BYOD), Capacity Management, E-mail Management, End Point System Management, Incident Service Desk Management, Logical Access Procedure Network Management, Password Management, Patch Management, Application Management, Application Change Management, Infra Change Management IT Governance Training Policy document is meant to be published on the intranet of RHFL and/or any other forum as decided by the management of RHFL. Anything not specifically stated in this policy document shall not be considered as implied in any manner.

1.12 For any clarifications related to these Policies document with respect to its interpretation, applicability and implementation, please write to **rhflitpopr@relianceada.com**

H. Annexure I – Exception Form

EXCEPTION FORM

Name of the requestor: Date: _____

Employee No: _____ Branch / Office Name: _____

Department: _____

Ph / Extn no: _____ PC Name: _____

Exception/s requested	**Policy Ref.**	**Guideline ref.**	**Granted (Y/N)**
(Requestor to maintain copy for audit purpose)			

Justification: (Pls be as elaborate as possible and highlight why alternative options, if any, are not possible)

Risk Mitigants(requestor to specify):

Residual Risk:

Risk	Risk Rating (High/Medium/Low)	Recommended Control	Effectiveness	Residual Risk	Remarks

Requestor's Signature: _____

I/ We understand and accept the residual risks mentioned above.

Approval of Information owner: (Reporting Authority)

Name: _____ Signature: _____ Date: _____

Approval of Requestor's Technology Head: (AVP & Above)

Name: _____ Signature: _____ Date: _____

Approval of Head–Information Security: (Please send the form to BISO for validation & approval)

Name: _____ Signature: _____ Date:_____