INSURANCE REGULATORY AND DEVELOPMENT AUTHORITY OF INDIA

INFORMATION AND CYBER SECURITY GUIDELINES

VER– 2.0

APRIL, 2026

TABLE OF CONTENTS

1.0 General Guidelines 5

1.1. Purpose 6

1.2. Scope 6

1.3. Principles and Objectives 7

1.4. Applicability 8

1.5. Governance 9

1.6. Roles and Responsibilities 10

1.7. Acceptable Usage 19

1.8. Risk Management 211

1.9. Exceptions 23

1.10. Compliance 25

2.0 Security Domain Policies 27

2.1. Data Classification 28

2.2. Asset Management 40

2.3. Access control 49

2.4. Human resource security 58

2.5. Information Systems acquisition and development 63

2.6. Information systems maintenance 70

2.7 Mobile security policy 79

2.8 Bring your own device (BYOD) policy 81

2.9 Change Control 86

2.10 Incident and problem management 90

2.11 Network Security 97

2.12 Cryptographic Controls 103

2.13 Business Continuity Management and Disaster Recovery 106

2.14 Third party service providers 113

2.15 Physical and environmental security 119

2.16 Monitoring, Logging and Assessment 131

2.17 Legal and Regulatory Compliance 138

2.18 Situational Awareness 141

2.19 Cloud Security Policy 142

2.20 Cyber Resilience 155

2.21 Email Security 159

2.22 Work from Remote Location 161

2.23 Dealing room operations 164

2.24 IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 167

Annexure A 171

Annexure B- RACI Matrix 172

Glossary 174

DISTRIBUTION LIST

NO.	NAME OF THE USER
1.	Chief Risk Officer (CRO) -
2.	Chief Information Security Officer (CISO)
3.	Members of The Risk Management Committee
4.	Information Technology (IT) Team
5.	Any other User / Entity authorized by CISO
6.	End Users

1.0 GENERAL GUIDELINES

The IRDAI Information and Cyber Security Guidelines are issued in order to enable Regulated Entities (REs) or Organizations to create their Information & Cyber Security Policy and put in place effective Governance Framework in line with these guidelines for implementing their Policy based controls to protect organization's Critical data and Information Assets.

1.0 General Guidelines

1.1. Purpose

Organization's Information and Cyber Security Policy (ICSP) plays an important role in identifying the responsibilities and establishing the goals for consistent and appropriate protection of the organization's Critical data and Information Assets.

By implementing ICSP, the Organization shall 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. Further, through the ICSP, the organization will be able to consistently establish and maintain controls for ensuring confidentiality, integrity and availability of all information assets. Additionally, it also safeguards working environment for its employees and partners who facilitate and support the goals in services.

Vision: To enable Regulated Entities to design their own Information and Cyber Security policy to provide a user-centric trusted and secure set of resources and environment to employees to conduct business, while ensuring protection of organization's information assets including customer data.

Mission: Ensuring the security of all Organization's 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 Organization's business purpose or operations. Information Assets include business data, system logs, servers, desktops, network equipment, network media, storage media, paper, people etc.

Organization'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.

1.3. Principles and Objectives

The ICS Policy and supporting procedures of the Organization shall be based on the following principles and objectives as set below:

1. **Information Protection** - Information Assets will be protected at a level commensurate with their value and the risk of loss to the organization. Protection should stress the confidentiality, integrity, and availability of Information Assets.

2. **User Authentication and 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

3. **Accountability** - Users and Custodians of Organization's Information Assets are responsible for the appropriate use, protection and privacy of these assets. All Organization's system will generate and maintain appropriate audit trails to identify Users, IT assets and document security-related events and processes.

4. **Availability** - Information Assets must be available to support Organization's business objectives. Appropriate measures must be taken to ensure the timely recovery of all information and access by authorized individuals

5. **Integrity** - Information Assets must be adequately protected to ensure completeness and accuracy. Validation measures will allow detection of inappropriately modified, deleted, or corrupted information

6. **Trust** - Partners, vendors and service providers must demonstrate ability to meet or exceed Organization's security requirements and justify confidence in their ability to secure Organization's Information Assets. Trust becomes increasingly important when Organization's Information Assets are shared with business partners and service providers

7. **Continuity** - Organization must demonstrate the ability to maintain continuity of operations from business and technology perspectives. All information assets and related policies and procedures of Organization, shall be evaluated from a continuity perspective to support Organization's business objectives. Partners, vendors and service providers must all demonstrate the ability to meet or exceed Organization's continuity objectives at all times

8. **Cyber Security Resilience**- To enable effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through appropriate legislative intervention

9. **Regulatory Compliance-** To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem

1.4. Applicability

These guidelines are applicable to all Insurers including Foreign Re-Insurance Branches (FRBs)* and Insurance Intermediaries regulated by the Insurance Regulatory and Development Authority of India (IRDAI).

Insurance Agents, Micro-Insurance Agents, Point of Sale Persons and Individual Surveyors will not fall under purview of these guidelines. However, it is responsibility of Insurers to ensure that these entities follow minimum security framework as defined under Insurers' Board approved policy in this regard.

These guidelines are applicable to all data created, received or maintained by Regulated Entities wherever these data records are and whatever form they are in, in the course of carrying out their designated duties and functions.

The Applicability of NIST Framework to All Regulated Entities is provided in Annexure – I.

The classification of Insurance Intermediaries based on gross insurance revenue is provided in Annexure- II.

The Auditors report comprising of Audit Summary, overall findings, non-compliances, risk rating and the Audit checklist is provided in Annexure – III.

The Eligibility Criteria for the Audit firm is provided in Annexure- IV.

The Text of Audit Certificate to be certified by the Audit Firm is provided in Annexure – V.

The Text of Audit Certificate to be certified by the Audit Firm for FRBs is provided in Annexure – VI.

* For FRBs:

1. reference to the Board shall be as defined in Registration of FRBs & Lloyds Regulations as amended from time to time.
2. as long as governance responsibilities outlined in the specified committees are met at regional / controlling / head office for complying with these guidelines, they may not constitute committees at the branch level.
3. W.r.t to compliance with the provisions of guidelines or controls provided in the checklist (annexure-III), FRBs shall 'comply or explain', subject to a reasonably justifiable explanation, as a part of the supervisory process.

1.5. Governance

I. Target Audience

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

The implementation of this policy shall be the responsibility of various departments 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.

II. Governing Board

The Information and Cyber Security Policy (ICSP) of Organization shall be governed by the Information Security Risk Management Committee (ISRMC) comprising of the Chief Risk Officer (CRO), Chief Information Security Officer (CISO), and Representatives / Heads of IT, Operations, Finance, Legal, Compliance, HR, Admin, etc. 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. The ISRMC shall meet at least on a quarterly basis with the quorum of CISO and at least two members.
The implementation and enforcement of the ICSP shall be facilitated by the CISO and governed by the ISRMC.

III. Ownership and interpretation

The ICSP is owned and maintained by the CISO. CRO will assume the responsibilities of the CISO in case decision needs to be made in the absence of the CISO.

IV. Review Frequency

This policy shall be reviewed on an annual basis and if required updated by the CISO 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 an organization 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 organization 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.

1.6. 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. **Board of Directors**

The Board shall

- Play a proactive role in ensuring an effective Information and Cyber Security governance and shall be ultimately responsible for the information security of the organization.

- Approve Information and Cyber Security Policy
- Approve and review the Cyber security strategies and ensure that they align with the Organization's overall objectives.
- Provide sufficient budget for Information and Cyber security keeping in view the current/emerging threat landscape and ensure that the budget is proportional to the organization's risk appetite.
- Approve appointment of Chief Information Security Officer (CISO) who shall be responsible for driving and managing Information and Cyber security program.
- Receive quarterly inputs on matters related to Information Security.
- Receive the status of non-conformities observed in the annual cyber security assurance audit report and risk report.
- Approve timelines for closure of gaps observed and ensure that gaps are closed within 12 months of reporting.

2. 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 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 shall represent information security related event / issues and initiatives at the Risk Management Committee.

3. Chief Information Security Officer (CISO)

A sufficiently senior level official with requisite technical background and expertise* shall be designated as CISO. The CISO should report directly to the top executive overseeing the risk management function or in his absence to the CEO directly and shall assume overall responsibility for governance and monitoring of Information Security. The CISO shall not have direct reporting relationship with the Head of IT Function and shall not be given any business targets. The CISO should have a reasonable minimum term and should be adequately staffed with people having relevant technical expertise*.

*The technical expertise herein means the ability to understand and evaluate information systems and associated IT/Cyber risks.

The CISO shall be responsible for carrying out, at a minimum, the following functions:

- Definition and periodic review of the ICSP after due approvals from the ISRMC
- Definition and periodic review of IS standards including IS Procedures / Templates, BCP / DR standards, Application security, Vendor risk assessment standards, Vendor classification standards, Technology Risk Assessment (TRA), etc.
- Conducting and coordinating both internal and external IS reviews and assessments
- Briefing to the ISRMC and the Board.
- Shall be Permanent invitee to IT Steering Committee**.** Be responsible for ensuring reporting of all cyber security incidents to Cert-In and other relevant stakeholders / Regulators within stipulated time limit.
- Be responsible for ensuring periodic participation of organization in national/ sectoral/ organizational Cyber Security Exercises and drills such as Cert-In Cyber Security Exercises Program
- Be responsible for planning and conducting regular cyber security exercises and drills on crisis situations and incorporate the learning outcomes into improving policies and plans.
- Conducting 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
- Liaising with the business teams to define the roles within each application under their purview depending upon the business requirements
- The CISO may engage external forensic experts who are certified as well as competent for the job as and when required.
- The CISO shall be responsible for presenting / escalating the budgetary requirements for resources as well as IS reviews to the CRO
- The CISO in consultation with senior management shall inform Chief Risk Officer about any security incidents and breaches, deemed necessary for notifying relevant regulatory authorities
- The CISO shall review and comment on each of requested exceptions to information security policies, standards and procedures.

- The CISO shall ensure effective functioning of the security solutions including SOC, DLP, etc. deployed.

- The CISO shall be responsible for driving cyber security related projects within the Organization including evaluation and selection of security solutions and controls.
- The CISO shall be responsible for managing and monitoring of the Security Operations Center (SOC) 24*7.

  The CISO shall receive escalations from SOCs on critical / open IS incidents based on their monitoring activities. Also, the CISO shall provide guidance and oversee the tracking and closure of such incidents. The CISO shall be responsible to highlight the status of critical incidents to ISRMC.
- The CISO shall be empowered and responsible for conducting risk assessment of the Infrastructure and Applications.
- The CISO shall develop and implement Scenario based Incident Response plans to deal with Cyber crises, contingencies and disasters, attacks on IT systems etc.
- The CISO shall be responsible for complying with guidelines issued by Cert-In from time to time.

4. Chief Technology Officer / Head of IT Function

- CTO shall enable and support implementation of the security related technology and processes within the organization in consultation or agreement with CISO.
- CTO shall ensure that information technology and processes are in line with the IS standards defined by the CISO.
- CTO shall ensure information security considerations are integrated into planning and budgeting cycles, enterprise architectures, Information Systems design, development and acquisition/system development life cycles.
- CTO shall ensure that all identified vulnerabilities through internal/external audits or Risk Assessment are remediated in a timely manner and as per documented policy including ensuring of updated systems to avoid EOL / EOS issues in the IT environment.

5. Chief IT Security Officer (CITSO)

- The requirement of having a CITSO role is done away with, however, organizations to ensure all functions envisaged to be done by the erstwhile CITSO are under the job definitions of CISO/CTO as may be applicable;

6. Chief Security Officer (CSO) / Admin / Head Administration

The Chief Security Officer shall be responsible for:

- Admin with adequate support from IT / IS team shall be responsible for implementing and maintenance of physical and environmental security controls
- 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 employ

The roles and responsibilities prescribed above are baseline governance controls, however, REs may adopt enhanced controls commensurate with their risk profile, size, and complexity.

7. 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 joinees induction program. HR shall sensitize new joinees 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 joinees 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 IS 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 joinees to ensure that the people with the right background and a healthy perspective join the organization
- HR shall cooperate with the 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.
- HR shall document, incorporate and communicate a formal disciplinary process to take action against employees / critical vendor employees who have committed an information security breach.

- HR shall ensure that InfoSec responsibilities of employees and vendor employees at time of termination / change of employment are clearly defined and communicate

The roles and responsibilities prescribed above are baseline governance controls, however, REs may adopt enhanced controls commensurate with their risk profile, size, and complexity.

8. Administrative / Admin Team

- 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 CISO to drive the organization towards building a pro-InfoSec environment and also assist them in obtaining relevant certifications related to the same.

The roles and responsibilities prescribed above are baseline governance controls, however, REs may adopt enhanced controls commensurate with their risk profile, size, and complexity.

9. ERM

- ERM shall provide the CISO with periodic updates of the status of the current IS Risks and actions needed if any.
- ERM team shall work with CISO 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.

10. Internal Audit

- The internal audit and information security functions shall work synergistically: the information security function shall design policies, procedures and standards 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.
- The Internal audit function shall keep the audit committee apprised of emerging risks and effective ways to address them.
- 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 controls in operations

11. Legal & Compliance Team

- Compliance team shall ensure that the organization is conducting its business in compliance to IRDAI and other applicable regulations
- Compliance team shall communicate applicable regulatory/legal guidelines and requirements including any changes related to Information and Cyber Security with Board/Risk team/CISO/CRO
- Legal & Compliance team shall be responsible for engagement with Legal, Statutory, Local enforcement agencies and Government agencies for communicating cyber security status and incidents.

12. Functional Head/Business Owner

- Define and communicate the importance of cybersecurity within the respective business unit/function

- Ensure the implementation and adherence to cybersecurity policies, procedures, and guidelines by all team members.
- Collaborate with the organization's Chief Information Security Officer (CISO) to assess and address specific cybersecurity risks associated with the business unit/function.
- Facilitate regular cybersecurity awareness training for employees within the business unit/function.
- Report and escalate cybersecurity incidents promptly to the designated incident response team.
- Functional teams shall designate a suitable and qualified team member who will be responsible for reporting the incidents & effectiveness of security control to Information Security Function
- Be primarily responsible for risk, data security and access of their respective Third-party partners and vendors
- Be responsible for conducting security assessments and audits of their respective Third-party processes / sites

13. Information Security Risk Management Committee (ISRMC)

- The Committee shall review and recommend to the Board necessary changes to the high level ICSP. The Committee shall approve standards and procedures in line with the Board-approved ICSP.
- The Committee shall refer to the RMC on any matters related to IS Risk Management that come to its attention that are relevant for the RMC.
- The ISRMC shall obtain periodic inputs from the CISO which shall include list of security incidents – root cause for the same as well as remediation actions taken.
- The ISRMC shall report the status of non-conformities observed in the annual cyber security assurance audit report along with timelines for closure of gaps observed, to the RMC, which in turn will take to the Board serious non-conformities, if any, observed.
- 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.
- The Committee shall provide relevant periodic assurances to the Risk Management Committee (RMC) on a quarterly basis.
- The Committee shall provide recommendations to the RMC on the organization's IS risk profile, appetite and ensure that an appropriate level of internal controls in line with its risk appetite and oversees the identification, management and reporting of IS risks to the appropriate Committees.

- CISO shall be convener of the ISRMC.

14. IT Steering Committee (ITSC)

- The Organization shall establish a ITSC with representation at senior management level from IT and Business functions.
- The roles and responsibilities of ITSC, inter alia, shall be
    - Assist the Board in developing the IT strategy for the Organization in alignment with business needs;
    - Ensure implementation of a robust IT architecture meeting statutory and regulatory compliance;
    - Ensure Updated IT Architecture diagram is maintained representing all IT components on prem/co-hosted/cloud components
    - Ensuring all IT Related SLAs/SOWs are in alignment with regulatory requirements and periodic review of SLA monitoring process including review of processes adopted for access review for accesses granted to third party service providers/external IT vendors etc.
    - Ensure effective implementation and governance of business continuity and disaster recovery frameworks;
    - Monitor the effectiveness of controls established to protect policyholder data within IT systems;
    - On Aspects of IT Procurements or projects, software license subscriptions, Saas Service subscriptions, tools procurement etc. which have a bearing on Information Security, the Committee needs to obtain the inputs from CISO function to ensure IT and IT Security are aligned on such decisions.
    - Update RMC & CEO periodically on activities of ITSC.
- The ITSC shall meet at least on a quarterly basis. The Chief Technological Officer shall be the convener of ITSC.

15. Control Management Committee

- The requirement of Control Management Committee (CMC), a board level committee, is done away with, however, Organizations are required to ensure that all functions envisaged to be done by the erstwhile CMC are part of Risk Management Committee (RMC) terms of reference.

16. Independent External Expert (IEE)

- Considering the importance of Cybersecurity in rapidly changing technological landscape, one or more Independent External Expert (IEE) having substantial IT and/or Cybersecurity expertise in managing or guiding IT/Cybersecurity related initiatives or projects, shall be a part of RMC.

1.7. Acceptable Usage

Acceptable Use Policy (AUP), shall be a document designed to establish clear guidelines for the responsible and secure use of digital resources. This said policy must address key facets of digital landscape, including the acceptable usage of organization-provided IT assets, personal devices for official purposes, intellectual property, organization email facilities, information processing facilities, and social media etc. Disciplinary action shall be taken for any willful violation to the above Guidelines.

The Acceptable Usage Policy prescribed here is a minimum mandatory security requirement. However, the REs are free to implement enhanced controls.

The Organization shall, as a part of their Board-approved ICSP, have Guidelines related to the usage of the following:

1. Acceptable usage of Organization provided IT assets
2. Acceptable usage of personal devices for official purposes (it will be disallowed unless explicitly approved by your Organization)
3. Acceptable usage of intellectual property
4. Acceptable usage of organization email facility
5. Prevention of misuse of information processing facilities
6. Acceptable usage of social media

a. 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 "Acceptable usage of Social Media".

- Employees should 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 Organization 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, should be forwarded to the Organization's Compliance team and corporate communication team for prior approval.
- Media Forum should not be used to report a service fault or to make a complaint

b. Guidelines for usage of social media by employees for personal purposes:

Organization's reputation is closely linked to the behavior of its employees, and everything published reflects on how Organization is perceived. Social media should be used in a way that adds value to the Organization's business. Considering the following points may help avoid any conflict between personal use of social media and an employee's employment at Organization-

- When subscribing to or posting information to an online/internet networking service, Organization personnel must not use their Organization email address or other Organization 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 should be identified as your own individual and personal interactions. These personal interactions should not in any way be assigned to Organization or written in such a way that they could be interpreted as corporate Organization 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 Organization must include a simple and visible disclaimer such as "The postings on this service are my own personal views and not those of Organization 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 Organization. No form of critique or comment on Organization or its business should be made on personal websites or social networking platforms.

- When using social media for personal purposes, employees must not imply they are speaking for Organization. The use of the official e-mail address, official logos or other identification should be avoided, and it should be made clear that what is said is not representative of the views and opinions of Organization.
- Employees should comply with other Organization policies when using social media. For example, staff should be careful not to breach Organization's Confidentiality and Information Security, or the Employee Code of Conduct. If in doubt, don't post it.
- Staff should be mindful of their privacy settings.
- Employees should be aware that if they break the law using social media (for example by posting something defamatory), they will be personally responsible.
- Employees should be aware that by revealing certain details they might be more vulnerable to identity theft.
- The CISO 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 the Organization.

1.8. Risk Management

IS Risk Management being necessary in order to maintain Organization's competitive advantage via positive image and reputation as a secure, discreet, and trustworthy organization. Risk must be managed to prevent financial loss, loss of customer confidence, and/or loss of operating licenses. Risk Management has the following objectives:

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

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:

I. Risk Assessment Scenarios

Organization shall perform Risk Assessment periodically at least annually and prior to the following scenarios/circumstances:

- Introducing major new technologies and initiatives.
- Using the services of external service providers (e.g. when outsourcing, off shoring or using cloud service providers)
- Permitting access to organization's critical systems (including those under development) by external individuals (e.g. consultants, contractors and employees of external parties)
- Granting access from external locations (e.g. employees' homes, external party premises or public places)

II. Target Environments

Risk Assessment shall be performed for the following environments:

- Business environments (e.g. administration offices, operating floors, call centres etc.)
- Business processes (e.g. processing high value transactions, handling customer records)
- Business applications (including those under development and being used in production)
- Information systems and networks that support business processes
- Specialist systems that are important to Organization (e.g. systems that support or enable critical infrastructure)
- Employees, staffs, third party vendors

Target environments shall be subject to risk assessment:

- At early stage of in their development

- Prior to significant changes
- When considering if they need to be outsourced to an external party

III. Risk Treatment

a. Organization shall ensure adequate security controls are put in place to responds to the risks to the assets.
b. Information risk treatment actions (together with residual risk) shall be detailed in Risk Treatment Plan, that is Communicated to the relevant business owner, Signed off by the relevant owner and at least one representative of executive management, compared with information risk assessments conducted in other areas of an Organization.
c. Results from information risk assessments conducted across Organization shall be reported to owners of business environments and executive management (or equivalent), used to help determine programs of work in information security (e.g. developing an information security management system (ISMS), performing remedial actions and establishing new security initiatives), integrated with wider risk management activities (e.g. managing operational risk)

IV. Continuous Monitoring and review

a. Organization shall perform risk assessment periodically at least annually according to the risk assessment methodology report.
b. Organization to verify the adequacy of existing controls, residual risk and acceptable level of risks.
c. Implemented controls shall be monitored and control effectiveness measured
d. Any new risks arising due to significant changes made to the assets or business processes shall be identified.

1.9. Exceptions

I. Need for exceptions:

In certain situations, exceptions to the established cybersecurity policies may be necessary to accommodate specific business needs, technological advancements, or unforeseen circumstances. However, any exception must be granted with the utmost caution and adherence to a formalized process

Prior to such a decision, the TRA shall be performed and appropriate approvals need to be obtained. Exceptions shall not be universal but shall be agreed on a case-by-case basis, upon official request made by the information owner. The purpose of such a process is to ensure adequate analysis and conscious acceptance of the risk represented by non-compliance with a policy.

II. Exception grant and risk assessment methodology

Exceptions not exceeding three months shall be approved by the Chief Information Security Officer (CISO) of the organization. Exceptions exceeding three months shall be approved by the Risk Management Committee (RMC). Further, exceptions exceeding one year shall be approved by the Board of Directors of the organization

An organization shall have a formal process for grant of exception which shall include a detailed explanation of the specific policy or control for which an exception is sought, the rationale behind the request, the potential impact on security, acceptable tolerance limit and appropriate authority to approve exception requests.

Risk Assessment Process - A risk assessment must be completed and approved to support any decision not to comply with any requirement of Organization's Information Security Policy. All policy exceptions must be fully documented, reviewed and retained as long as the exception exists. The documentation shall address:

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

Any exception request exceeding 12 months must undergo a reassessment and re-approval process. All exceptions granted should formally document risk associated with granting such exceptions.

III. Executive Approval

Any changes to the Information Security environment which expose the organization towards inordinate risks which cannot be mitigated by putting in place appropriate controls, may be accepted after considering IS team's opinion on the risks.. Executive approval signifies:

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

IV. Emergency exceptions

Events such as Pandemic, War, Emergencies and Natural Disasters etc. unfold odd and exceptional situations necessitating workaround solutions so that services to customers and other stakeholders such as the Government, Revenue Authorities, Regulators and Public at large are not impacted. This necessitates careful deliberations on the new / revised emergency processes, personnel and technological changes that may pose challenges to the existing security policies of the Companies. A Crisis Management Committee needs to be formed during such events by drawing up resources from all key functions of the organization and deliberate on the revised processes, technology and personnel to operate and execute decisions. The Risk management function including the Information security function shall collate the risks in such situations and present the same for the approval of the Crisis Management Committee. The same shall be presented to the Risk Management Committee of the Board for ratification and further directions, if any.

The Crisis Management Committee under the overall directions and guidance of the Board's Risk Management committee shall be vested with powers to devise changes to processes, systems, personnel and technology controls to ensure continuity of services. Information security compromises should be dealt with as exceptions and the enterprise shall devise risk mitigation controls to bring down the risks and shall eliminate such compromises once the business / affairs come into normalcy.

1.10. Compliance

An independent Assurance Audit shall be carried out by the Auditor every year. The annual Audit plan and the reports shall be presented to the Audit Committee / Risk Management Committee / Board of Directors / Principal Officer, as applicable, of the organization.

The Insurance Intermediary shall submit the Annexure – III along with compliance thereto and the comments of the Audit Committee / Risk Management Committee / Board of Directors / Principal Officer, as applicable, to the Insurer/s annually, within 30 days of completion of Audit by an CERT-In empaneled Auditor or Audit firm as prescribed under Annexure IV of the guidelines.

The Insurer shall ensure that the Insurance Intermediaries engaged by them comply with these guidelines during the currency of their engagement. Insurer shall have a Board approved policy in this regard.

The risk rating for entering into or continuing business with Insurance Intermediary as per Part-C under Section-I in Annexure III shall be as per the Board approved policy of the Insurer.

In case of Insurance Intermediaries which retain only insurer's data in physical form and do not hold any electronic database of the insurers' data or do not access insurer's systems, the Insurer shall obtain the necessary self-certifications in this regard on annual basis before entering into or continuing to carry on business with it.

The Foreign Reinsurance Branches (FRBs) where IT Systems are interfaced with overseas parent companies shall comply with Cyber Security Guidelines. The Auditor shall certify the same as per Annexure – VI and the same shall be submitted to IRDAI at the end of every financial year.

The Insurers shall submit their Audit Report (Annexure III) duly signed by the Auditor along with comments of the Board to IRDAI within 90 days from the end of financial year or within 30 days of completion of Audit, whichever is earlier.

Regulated Entities shall adhere to directions issued by Cert-In from time to time including relating to information security practices, procedures, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.

Also, Regulated Entities to educate security researchers about CERT-In's role as a CVE Numbering Authority (CNA), the Responsible Disclosure Framework, and the acknowledgement process administered by CERT-In.

Regulated Entities 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, Insurance Regulatory and Development Authority of India (IRDAI) or any other laws or acts as applicable. Also, Regulated Entities must take appropriate technical and organizational measures to comply with the provisions of Digital Personal Data Protection Act (DPDP) and rules made thereunder.

2.0 SECURITY DOMAIN POLICIES

This section is a guidance document for Regulated Entities to frame their own policies, specifying appropriate and adequate security controls along with the applicable standards. The policies shall encompass each of the security domains provided and shall be a part of their approved Information and Cyber Security Policy.

2.0 Security Domain Policies

Policy No.:	2.1
Policy Name:	2.1. Data Classification

1	**Purpose**	To provide a framework for information owners to determine and classify the sensitivity levels for the information that Organization uses, processes, and stores. The unauthorized disclosure, modification, accidental or intentional damage, or loss of sensitive Organization information could constitute a violation of laws and/or regulations, may negatively affect customers, and impact Organization'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	**Scope**	This policy applies to information systems, including IT applications, IT infrastructure and physical information channels, and the information assets that Organization uses, process, and stores using those systems. It also applies to the business processes and procedures at Organization regarding data processing. This policy applies to all individuals handling data as well as technology systems where Organization'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 security policy.

3	**Policy**	The Information Owner shall only classify information assets within their purview using one of the following four classification levels: • Public • Internal • 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. Organization 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.
3.1	**Data Ownership**	All information assets within Organization 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.
3.3	**Data Classification Process**	Information owners shall ensure that the information assets for which they are responsible are assigned a classification rating (Confidential, Restricted, Internal, and Public) 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 Organization.

3.3.1	**Confidential**	Personal or Organization information that is classified as highly sensitive by senior management or laws and regulations that impact Organization. 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 Organization, its brand and/or reputation, and its customers.
3.3.2	**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.
3.3.3	**Internal Use Only**	Will constitute of Information that is not intended for use by the public. This can include information posted on Organization intranet for employee use, such as phone directories or the Employee Handbook. Unauthorized disclosure of Internal Use Only information could moderately impact Organization, its brand and/or reputation, and its customers.
3.3.4	**Public**	Will constitute of Information that is approved for release to the public by Organization'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 Organization, its brand and/or reputation, and its customers.
3.3.5	**Technical Standards**	Technical standards should be based on the life cycle process defined below in this document. Section 3.5 'Lifecycle Processes' outlines the specific controls to protect the confidentiality and integrity of Organization's information assets.

3.4	**Lifecycle Processes**	
3.4.1	**Confidential Information**	
3.4.1.1	**Labeling Requirements**	A label of "CONFIDENTIAL" shall, at a minimum, be legible on every page of the physical or electronic document 1. Any device or object (including portable devices) that contains CONFIDENTIAL information shall be labelled as "CONFIDENTIAL". 2. Systems that contain CONFIDENTIAL information shall be identified and mentioned in "Asset Library". 3. Storage repositories that maintain CONFIDENTIAL information shall be known and controls implemented to effectively protect the information 4. Emails that contain CONFIDENTIAL information shall, at a minimum, contain "CONFIDENTIAL" in the subject line, header, or footer.
3.4.1.2	**Storage Requirements**	1. Storage environments shall require user authentication that can uniquely identify each user or administrator. 2. Storage environments shall be periodically reviewed and audited to help ensure that information is sufficiently secured. 3. Storage environments shall be monitored to help ensure that access control systems are functioning properly. 4. CONFIDENTIAL information shall be stored on Organization owned or controlled systems or on equivalently secured systems with which Organization has an approved partnership.
3.4.1.3	**Transfer Requirements**	1. When CONFIDENTIAL information is transmitted outside of the Organization 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.

		2. CONFIDENTIAL information entrusted to Organization by a third party shall be encrypted when sent over external network systems. 3. CONFIDENTIAL designations shall appear on the cover sheet of transmitted documents (i.e., facsimile transmissions). 4. Phone calls, SMS or electronic communications that discuss CONFIDENTIAL information shall be preceded by a statement about the sensitivity of the information involved. This may be achieved by labelling information or communications as per Traffic Light Protocol (TLP). 5. When distributing CONFIDENTIAL information via physical format (paper, disks, etc.), enclose the information in an envelope labelled "CONFIDENTIAL" even when delivered by hand. 6. Intellectual Property shall not be transmitted without prior authorization from the Information Owner.
3.4.1.4	**Tracking Requirements**	1. 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. 2. This access shall be audited by the Information Owner and deficiencies corrected in a timely manner
3.4.1.5	**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. Sensitive data or systems not regularly accessed by the Organization shall be removed from the network. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed
3.4.2	**Restricted Information**	

3.4.2.1	**Labeling Requirements**	1. 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 labelled as "RESTRICTED". 2. Systems, applications, and databases that contain RESTRICTED information shall provide a legible label of "RESTRICTED" on appropriate output or displays. 3. 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). 4. 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. 5. Emails that contain RESTRICTED information shall, at a minimum, contain "RESTRICTED" in the subject line, header, or footer
3.4.2.2	**Storage Requirements**	1. 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. 2. Storage environments shall require user authentication wherever possible that can uniquely identify each user or administrator, even for portable electronic devices. 3. RESTRICTED information shall be stored on Organization owned or controlled systems, or on equivalently secured systems with which Organizationhas an approved partnership. 4. Storage environments shall be periodically reviewed and audited to help ensure they are sufficiently secured. 5. Storage environments shall be monitored to help ensure that access control systems are functioning properly.

		6. 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.
3.4.2.3	**Transfer Requirements**	1. When RESTRICTED information is transmitted electronically outside of the Organization's network, including the Internet, it shall be sent over a secured channel or in encrypted form. 2. Encryption keys shall be managed and protected by authorized resources as defined in the Cryptographic Security policy. 3. RESTRICTED information transmitted electronically shall be accompanied by a caution to the recipient as to how the RESTRICTED information shall be handled and protected. 4. When transmitting RESTRICTED information via physical format (paper, disks, etc.), enclose the RESTRICTED information within double envelopes. The internal envelope shall be labelled "RESTRICTED". The external envelope shall have no special markings and shall be delivered by hand or as appropriate. 5. RESTRICTED designations shall appear on the cover sheet of transmitted documents (ex. facsimile transmissions). 6. 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 7. RESTRICTED information shall not be verbally communicated within insecure facilities. Individuals shall ensure that there are no unauthorized persons within earshot before conversation begins.
3.4.2.4	**Tracking Requirements**	1. 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. 2. This access shall be audited by the Information Owner and deficiencies corrected in a timely manner

3.4.2.5	**Disposal Requirements**	1. 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
3.4.3	**Internal use only Information**	
3.4.3.1	**Labeling Requirements**	1. INTERNAL USE ONLY information does not have any specific labelling requirements. However, if information or an information source is not labelled, at a minimum it shall be treated as INTERNAL USE ONLY. 2. A label of "INTERNAL USE ONLY" shall be legible on the first page of the file, document, or on the front of the device.
3.4.3.2	**Storage Requirements**	1. The storage environment shall require user authentication that can uniquely identify each user who accesses the information. 2. Appropriate controls shall be put in place to ensure that only authorized users get access to "INTERNAL USE ONLY" information.
3.4.3.3	**Transfer Requirements**	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
3.4.3.4	**Disposal Requirements**	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
3.4.4	**Public Information**	
3.4.4.1	**Labeling Requirements**	No labels required

3.4.4.2	**Storage Requirements**	No specific storage requirements
3.4.4.3	**Transfer Requirements**	No specific transfer requirements
3.4.4.4	**Disposal Requirements**	PUBLIC information shall be disposed off at the end of its retention period OR at the release of a related litigation or audit hold
3.5	**Data Privacy**	1. Personally Identifiable Information (PII) is information about a person that contains some unique identifier, including but not limited to name, email, contact details 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 2. Any incident of data privacy violation must be reported immediately to the concerned authority so that the exposure can be contained. Refer to Incident and Problem Management Policy.
3.5.1	**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: 1. Password 2. User details as provided at the time of registration or thereafter 3. Information related to financial information such as Bank account / credit card / debit card / other payment instrument details of the users 4. Physiological and mental health condition 5. Medical records and history

		6. Biometric information 7. Information received by body corporate for processing, stored or 8. Processed under lawful contract or otherwise 9. Call data records 10. Any PII which is not considered SPI as per the above categorization will be treated as OPI.
3.5.2	**Collection of PII**	1. Organization 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 2. Organization or any person on its behalf shall not collect sensitive personal information unless – • 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 3. While collecting information directly from the individual concerned, Organization 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 4. Organization 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.

		5. The information collected shall be used for the purpose for which it has been collected 6. Organization or any person on its behalf shall permit the users to review the information they had provided and modify the same, wherever necessary.
3.5.3	**Storage, Transfer & Destruction of PII**	1. 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. 2. 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
3.5.4	**Processing of PII**	1. The entire customers' / employees' data shall be classified as per "Asset Management Procedure" 2. Personal data of customers/employees shall be securely stored, in manual or electronic form, and in accordance with the IT Act. 3. Personal data of customers/employees shall not be stored for longer than is required unless otherwise mandated by any law. 4. Personal data of customers/employees shall be used for the purpose for which it has been collected. 5. Access to the sensitive data shall be provided strictly on the basis of need to know. 6. Backup of sensitive data on a removable storage media shall be kept in safe and secure environment.
3.5.5	**Disclosure of PII**	1. If any of the Organization's customer/employee requests to view his/her own sensitive information collected, it shall be made available.

<table>
<tr><td></td><td></td><td>2. Organization shall not disclose an individual's personal data outside Organization except:

• When Organization expresses consent to do so, or in circumstances as agreed between Organization and the individual
• When necessary, to our regulatory bodies and auditors
• When Organization is required or permitted to do so by law
• To any persons, including insurers and lenders who supply benefits or services to the individual
• To fraud prevention agencies where required
3. Data protection tools like data loss prevention, digital rights management etc. shall be implemented to prevent unauthorized disclosure of sensitive data.</td></tr>
<tr><td>3.6</td><td>RACI Matrix</td><td><table><tr><th>Responsible</th><th>Accountable</th><th>Consulted</th><th>Informed</th></tr><tr><td></td><td></td><td></td><td></td></tr></table></td></tr>
</table>

Policy No.:	2.2
Policy Name:	2.2. Asset Management

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 Organization and achieve efficient and effective service delivery.
2	**Scope**	1. This policy applies to all information systems being used by Organization or involved in creation, storage, transmission or destruction of Organization'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 ▪ Information – Digital asset & non-digital assets 2. Any individual handling Organization's information assets in any form shall comply with this policy.
3	**Policy**	Organization's information assets including hardware, software and physical assets used in the Organization's physical environment and virtual premises such as hosting sites, service provider premises etc. shall be managed in accordance with the information asset protection asset i.e. from acquisition to its disposal. Any breach of this policy shall be considered as an incident and shall be treated objectives established in this policy throughout the lifecycle of the as per the incident management policy.

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: 1. Data Information systems/equipment containing the data including paper format on which data might be stored in printed form. 2. Data will be classified as per data classification policy. 3. 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
3.2	**Lifecycle Processes**	
3.2.1	**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.
3.2.2	**Asset Tracking**	

3.2.2.1	**Asset Labeling**	1. Every asset shall be marked for identification and inventory control. An appropriate set of procedures for asset labelling and handling shall be developed and implemented in accordance with the classification scheme(s). This shall include: • responsibility of the asset owner to assure/confirm classification and labelling, and subsequent handling consistent with that label; • classifications that cover all information processing facilities and information in all forms and media; • procedures for establishing ownership and chain of custody; and • procedures for logging and reporting security incidents associated with the asset. 2. 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.
3.2.2.2	**Asset Inventory and Documentation**	1. A comprehensive inventory of all information assets shall be maintained. 2. Each asset shall be clearly identified individually and (if appropriate) collectively in combination with other assets to form an identifiable information asset. 3. The asset inventory shall include all information necessary in order to recover from a disaster. 4. 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 5. Software inventory tools shall be utilised throughout the organization to automate the documentation of all software on business systems. 6. Software applications or operating systems currently supported by the software's vendor shall be added to the organization's authorized software inventory and unsupported software shall be tagged as unsupported in the inventory system. 7. The asset inventory shall be accurate, up to date, consistent and aligned with other inventories 8. For every asset Organization shall define service components or other items (Configuration Items) which are required to deliver or support one or more IT services. 9. Configuration Items (CI) shall be grouped, classified and identified in a way such that they are manageable and traceable throughout the service life cycle. 10. 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. 11. Status maintenance of CIs shall be consistently recorded and kept updated. 12. Organization'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
3.2.2.3	**Authorization Inventory**	1. The asset inventory shall contain details of authorization mechanism for all information assets

		2. For Organization-owned assets, the authorization record shall consist of the owner and the features of the asset used to authorize the asset to the Organization's network such as the network interface media access control (MAC) address or the IMEI number. 3. For non Organization-owned assets, the authorization record shall consist of parameters used for two factor authentication such as username and password, token ID or biometric record.
3.2.3	**Asset Use**	1. All Organization assets shall be used as per the 'Acceptable Usage' of assets covered in Section 1.7 of General Guidelines. 2. Organization's 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. 3. 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. 4. Assets shall be transferred among Organization's 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. 5. 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. 6. Assets assigned to consultant/temporary staff/third party vendor shall be linked to them as primary user and an Organization's employee as secondary user. However, it is the responsibility of the secondary user to monitor the activities of primary user. 7. Insurance companies shall use client certificates to authenticate hardware assets connecting to the organization's trusted network. 8. Port level access control shall be utilised, following 802.1x standards, to control the devices that can authenticate to the network

		9. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network. 10. 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. 11. Assets shall not be taken out of Organization's premises without appropriate authorizations. In scenarios where the asset may need to be taken out of Organization's premises for repairs / replacement appropriate authorizations shall be taken after ensuring that the data contained in the assets has been securely erased. 12. Employees who are possessing Organization provided mobile devices such as laptops, tablets, smart phones will have authorization to carry asset outside office premises. 13. IT assets shall be hardened as per the hardening guidelines laid down in the 'Information Systems Acquisition and Development' section of this policy – 3.1.1.1' 14. All assets requiring periodic maintenance shall be covered under appropriate Annual Maintenance Contracts (AMCs) which shall be renewed and kept current at all times. 15. Physical assets sent out of Organization's premises for maintenance purposes shall be checked against the gate pass. 16. IT team shall ensure that internal hard drives are either removed and kept securely or data is backed up and securely wiped from the hard drive before physical assets/hardware is sent out of Organization's premises to asset maintenance vendors

3.2.4	**Return of Assets**	1. All employees and external party users shall return all organization assets in their possession upon termination of their employment, contract or agreement. 2. The termination process shall be formalised to include the return of all previously issued physical and electronic assets owned by or entrusted to the organization. 3. Provide clearance for relieving once assets are received and access deactivated
3.2.5	**Transfer of physical media**	To prevent the unauthorized disclosure/dissemination of critical business information assets while in transit, the respective custodian shall ensure by verifying that: o Reliable transport and Controls are in place to ensure integrity and confidentiality of physical media. o A list of authorized couriers should be agreed with management; o Packaging is sufficient to protect the contents from physical damage. o All employees and third-party staff carrying media are required to ensure its protection from theft, weather conditions and damage during transit. o Logs shall be kept, for identifying the content of the media, the protection applied as well as recording the times of transfer to the transit custodians and receipt at the destination. Information asset owners shall be responsible for ensuring the implementation of the specified security controls on all the assets owned by them.

3.2.6	**Asset Disposal**	1. All assets and media containing critical and sensitive information shall be disposed in a secure manner by incineration or shredding, or erasure of data for use by another application within the organization; 2. Assets shall be disposed if: o The asset has reached end of life o The asset does not suit the environment 3. Critical infrastructure elements which need to be disposed off shall be approved with valid justification by the CTO and CFO. 4. Finance department shall also be informed as and when an asset is disposed off. 5. 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. 6. A register for all disposed / scrapped assets shall be maintained. 7. A process shall be put in place for media formatting 8. Damaged devices containing sensitive data shall require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded
3.2.7	**Management of removable media**	1. Asset custodians shall ensure media is physically protected to prevent interruptions to business activities and damage to critical business information assets. 2. Media shall be stored in a safe and secure environment. 3. A listing of all official media in use shall be maintained and reviewed on a regular basis. 4. Physical media containing information related to Organization shall be strictly monitored during active use and securely disposed as per the Asset Management Procedure when no longer needed. 5. Authorization shall be required for media removed from the organization and a record of such removals shall be kept in order to maintain an audit trail;

		6. In case of confidential data, cryptographic techniques shall be used to protect data on removable media;
3.3	**Loss / Theft of asset**	1. In case of loss / theft of personal device with access to Organization's Information assets, the employee shall report the same immediately. 2. The IT function shall be responsible to immediately revoke all access to Organization's Information Assets through the device and shall attempt to remotely wipe off Organization data from the device. 3. 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.
3.4	**RACI Matrix**	

Responsible	Accountable	Consulted	Informed

Policy No.:	**2.3**
Policy Name:	**2.3. Access control**

1	**PURPOSE**	1. To provide a set of practices for access to Organization's information and information systems (Operating Systems, Applications, Databases, Network Equipment and others). 2. Access controls pertaining to Organization'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	**SCOPE**	1. 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. 2. 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. 3. Both physical and logical access controls shall be implemented and maintained to protect information assets against unauthorised access. 4. This policy applies to all users such as employees, contractors, service providers / visitors accessing Organization's information assets.
3	**POLICY**	1. All user accesses to Organization's information assets shall be specifically and individually authorized based on business need. Security controls shall ensure that only authorized individuals can access Organization's information assets. 2. 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.

		3. Any breach of this policy shall be considered as an incident and shall be treated as per the incident management policy.
3.1	**User Identification and Accounts**	1. 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. 2. Each User-ID or account on Organization's 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. 3. 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.
3.2	**Group/ Generic User-IDs**	1. 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. 2. 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.

3.3	**User-ID Creation and Maintenance**	1. User-IDs shall be non-transferrable, and individuals shall not have multiple accounts within the same computing environment. 2. Access to Organization'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. 3. 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. 4. 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. 5. 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. 6. 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. 7. The password requirements for all user accounts shall follow the password standards as defined in the 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. 8. Users shall be required to change their passwords at the first log-on and change their passwords once in 45 days

		9. A record of previously used passwords shall be maintained to prevent re-use. Further, password files shall be stored separately from application system data. 10. 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. 11. The department heads shall maintain a central record of access rights granted to a user ID to access information systems and services 12. 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.
3.4	**User Authorization**	1. Users shall be authorized on Organization's information systems at the following levels: • Physical access • Network • Infrastructure • Endpoints • Applications • Cloud (where applicable) 2. 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. 3. Users shall be authenticated and authorised by a domain policy server. 4. 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. 5. All network and network services in Organization shall be identified and documented. Logical access to all network equipment shall be restricted to authorized users only.

		Appropriate security controls shall be used to restrict access to the IT systems of Organization. 6. 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. 7. Applications shall support integration with the enterprise identity management system 8. If the authorization request comes from a Organization-owned asset (device/network), single factor authentication will suffice. In case the authorization request comes from a non-Organization asset (device/network) two-factor authentication will be mandatory. 9. Applications hosted on the Cloud shall accept a user authorization record validated by a Organization-owned authorization service or require two factor authorization as stated in (6) above. 10. The access requirements shall be identified by Business Owner. 11. Respective Business Heads shall ensure that level of access granted is appropriate to Organization's purpose. 12. Users shall be required to re-authenticate themselves after a specific period of inactivity. 13. Organization shall establish process for granting access based on emergency. 14. Organization shall establish methods to prevent unauthorized access by other groups into individual files and department-shared files.
3.5	**Privileged User Accounts**	1. 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 includes (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. 2. Privileges associated with each type of information system such as Operating System, Business Applications, Databases, and Network elements shall be identified and documented. 3. 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. 4. Privileges shall be allocated to individuals on a 'need-to-have' basis in strict adherence to the authorization process for privilege access. 5. 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. 6. 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 2.16 Monitoring, Logging and Assessment for further details on logging and monitoring of privileged User-IDs. 7. 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. 8. Audit logging of system activities performed by privileged users, shall be maintained. Audit or management review of the logs shall be conducted 9. Sharing of privileged IDs and their access codes shall be prohibited 10. Vendors and contractors shall be disallowed from gaining privileged access to systems without close supervision and monitoring. Business justification for the same shall be documented.

		11. An authorization process and a record of all privileges allocated shall be maintained 12. Rules governing the installation of software by users shall be established and implemented.
3.6	**Secure log-on**	1. The Log-on process shall not provide any information that would aid an unauthorized user to successfully Log-on. 2. Log-on data shall only be validated after it has all been entered. 3. The log-on process shall not reveal which part of the log-on data is valid or invalid. 4. Account lockout shall be enforced by the log-on process after the retry limit is reached. 5. Log on process shall display a general notice warning that the computer should only be accessed by authorized user 6. Log of unsuccessful and successful attempts shall be maintained. 7. The log-on process shall not transmit passwords in clear text over a network 8. The log-on process shall terminate inactive sessions after a defined period of inactivity, especially in high risk locations such as public or external areas outside the organization's security management or on mobile devices;
3.6.1	**Review of access rights**	1. User access rights shall be reviewed at regular intervals and after any changes, such as promotion, demotion or termination of employment. 2. User access rights shall be reviewed and re-allocated when moving from one role to another within the same organization 3. Authorizations for privileged access rights shall be reviewed at more frequent intervals and changes to privileged accounts shall be logged for periodic review. 4. Privilege allocations shall be checked at regular intervals to ensure that unauthorized privileges have not been obtained
3.7	**Remote access**	1. Remote access to employees/ vendors/ contractors shall be provided on need to know and need to do basis only. 2. Remote access request for third party vendor/consultant shall be raised by the Organizationemployee responsible for the vendor

		/consultant engagement along with proper business justification. The request needs to be approved by sponsoring functional manager, Head – IT and Group CISO. If access is provided from non-Organization endpoints an exception shall be taken in this regards Head-IT and Group CISO. 3. Use of remote access software shall be restricted 4. No vendor user or general Organization user shall be assigned administrative privileges on the SSL VPN appliance. If third parties require privileged ID, monitoring of their activities shall be performed and the access shall be revoked immediately on their termination of association with Organization, 5. An expiration shall be placed on all third party user-IDs unless appropriate access review process is carried out and approval is given. 6. Remote access solutions must support strong, end-to-end encryption as mentioned in Organization's policy for Cryptographic Controls. 7. A remote log-on procedure shall be designed with consideration of encryption of information during its transmission. A secure network channel shall be established for remote access. 8. Organization security solutions and controls shall not be disabled or circumvented.
3.8	**Compliance and audit**	1. Periodic audits shall be carried out to ensure compliance with this policy. 2. Remote Access System Owners shall maintain evidence of all requests for granting remote access. 3. All notifications for initiating the revoking of remote access. 4. All evidence for granting, revoking, or changing remote access privileges shall be maintained in a repository such as Change Management System 5. SOP's and System Design documents for the remote access systems. 6. All changes to the remote access system configuration. 7. Patch upgrades performed on remote access systems.

		8. On a monthly basis, the system owner's shall ensure that the accounts active within the Remote access solutions are accurate. All discrepancies shall be resolved quickly.
3.9	**Access to program source code**	1. Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) shall be strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes as well as to maintain the confidentiality of valuable intellectual property. 2. Program source libraries shall not be held in operational systems. The program source code and the program source libraries shall be managed according to established procedures. 3. IT Support personnel shall not have unrestricted access to program source libraries. 4. The updating of program source libraries and associated items and the issuing of program sources to programmers shall only be performed after appropriate authorization has been received. An audit log shall be maintained of all accesses to program source libraries and program listings shall be held in a secure environment.
3.10	**RACI Matrix**	

Responsible	Accountable	Consulted	Informed

Policy No.:	2.4
Policy Name:	2.4. Human resource security

1	**PURPOSE**	1. To define Organization's desired practices concerning human resource security to ensure that: 2. The Human Resources function meets its requirements within the context of the corporate framework for the security of its information and equipment. 3. 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. 4. Employees, contractors and third-party user's entry, exit or change employment in an orderly manner.
2	**SCOPE**	1. Human resources are an integral element of Organization'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, organization reputation and regulatory non-compliance in not meeting customer confidentiality. 2. This policy shall apply to all employees, contractors and third-party users using Organization's Information Technology resources. 3. Human resource (HR) security is a part of personnel management and applies to pre-employment, duration of employment and termination of employment.
3	**POLICY**	1. Organization shall ensure that all users joining, moving within or leaving the Organization's 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 Organization 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.

		2. The policy aims to reduce risks arising from theft, fraud, or misuse of information and network assets/ facilities. 3. Any breach of this policy shall be considered as an incident and shall be treated as per the incident management policy.
3.1	**Prior to Employment**	1. 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 Organization shall understand their job roles and responsibilities. 2. 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 Organization. Information provided by the personnel, at the time of recruiting shall be subjected to verification procedures.
3.2	**On-Boarding and During Employment**	1. All employees, contractors and third party users of Organization'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 Organization's confidential and sensitive data. These terms and conditions shall state the organization's as well as the employee's responsibilities towards information security. 2. 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. 3. Processes and procedures shall be defined for reporting the violations of confidentiality agreements.

		4. 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. 5. All employees and contractors shall be properly briefed on their information security roles and responsibilities prior to being granted access to confidential information or information systems. Users shall understand and comply with the Information Security Management Policy and the other allied policies, as relevant to their roles and responsibilities. 6. Insurance companies shall ensure that employees and wherever relevant third-party users receive appropriate awareness/skills training and regular updates in organizational policies and procedures, as relevant to their job function. 7. All end users shall report suspected information security incidents and vulnerabilities as soon as possible to their controllers, designated official/system official. Unless required by law to disclose security incidents, employees shall not report incidents to external entities without authority. 8. Job rotation shall be enforced for employees in computer-related positions of trust. 9. Reliance/dependency on single person on key areas shall be avoided. Succession plans shall be developed for technical personnel deployed at critical locations. Adequate second line shall be ensured for development/maintenance activities 10. The punitive actions to be taken for violation of the information security requirements in the employment contract or the information security policy shall be as per the 'punitive actions' laid down as a part of the compliance section of the general information security policy. 11. Information Security Training and Awareness Programs shall be provided to all the employees, contractors and relevant third-party users of Organization systems in order to create consciousness about the information security policies and processes. 12. Organization Shall Periodically Participate in national/ sectoral/ organizational Cyber Security Exercises.

		13. 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. 14. 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. History and versions of training content shall be maintained. 15. Additional training shall be provided for leaders to understand their roles in the event of a security incident 16. Employees shall be periodically informed of their rights and duties in the organization in the form of Do's and Don'ts. This should also advise employees to refrain from using Organization assets for personal use. 17. Organization shall consider the higher level of monitoring the activities (particularly e-mail, administration and critical systems) of those users who are in the process of leaving the Organization. 18. All employees shall be provided with an anonymous reporting channel to report violations of information security policies or procedures
3.3	**Exit procedures**	1. Organization shall ensure that termination of employees, contractors and third-party users is performed in an orderly manner, and responsibilities are defined and communicated within Organization to ensure the same. 2. The assets of Organization available with terminated individuals shall be taken back and all their access rights (physical and logical) shall be removed immediately. 3. Organization 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. 4. 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. 5. Mechanisms shall be put in place to ensure that access granted to any employee or contractor is revoked at the time of termination of their employment / contract period with Organization or exit. Controls shall

<table>
<tr><td></td><td></td><td>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.
6. Any IS violations during the tenure of the employee shall be reviewed before the final sign off.</td></tr>
<tr><td>3.4</td><td>RACI Matrix</td><td><table><tr><td>Responsible</td><td>Accountable</td><td>Consulted</td><td>Informed</td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td></tr>
</table>

Policy No.:	**2.5**
Policy Name:	**2.5. Information Systems acquisition and development**

1	**PURPOSE**	To define the desired practises and ensure that information security is an integral part of information systems across their entire lifecycle.
2	**SCOPE**	This policy shall apply to all information systems where Organization's information assets are stored or processed and all communication and network connections through which Organization's information assets are transmitted. All Business Units or Departments using information technology shall comply with this information security policy. This shall apply to developing new software, customizing software and developing software that can be accessed or presented on a website.
3	**POLICY**	Organization's 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.
3.1	**Technology Standards**	
3.1.1	**Infrastructure standards**	
3.1.1.1	**Security requirement analysis and specifications**	1. 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. 2. 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. 3. Minimum Baseline Security Standards (MBSS) shall be developed and maintained and all information systems shall be configured as per such standards. 4. 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. 5. All information systems (server, routers, and firewalls) shall undergo hardening as per the MBSS before being commissioned for usage in the production environment. 6. The clocks of all relevant Information Systems within Organization's security domain shall be synchronized with an agreed accurate time source.
3.1.2	**Application security standards**	
3.1.2.1	**Security requirement analysis and specifications**	1. Applications shall be assessed for their security posture through security reviews before being commissioned for usage in the production environment. 2. Application security reviews shall be conducted based on application security standards 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.
3.1.2.2	**Application development**	1. A formal software development security framework shall be developed by the IS team. 2. 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. 3. A library of secure design patterns shall be built. Their consistent usage across projects shall be enforced, and it shall be ensure that new pattern requirements drive pattern

		development. Security reviews shall be focused on reviewing patterns and enforcement of their use. 4. 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 security policy. 5. All modifications (including configuration changes, changes to reports, etc.) to software packages shall be made in accordance with formal Program Change Control Procedures. 6. If the software is developed by a third – party, the following shall be done – • Organization shall ensure that software development processes followed by the third-party are in compliance to Organization's Information Systems Acquisition, Development policy. • As far as possible and practicable, vendor-supplied software packages shall be used without modification • Organization shall have appropriate licensing agreements and contractual requirements for quality and functionality of the application exist. • Appropriate documentation in form of product manuals or data sheets should be obtained from the third party to ensure that the security requirements of the Information Security policy are adhered to. • The consent of the vendor shall be obtained where a software package needs to be modified and the impact if the organization becomes responsible for the future maintenance of the software as a result of changes shall be assessed • The ownership of the source code shall be transferred to Organization or appropriate escrow arrangement shall be set up to ensure availability of source code to Organization during the usage of the provided software. • 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. • A formal methodology shall be defined and documented including security requirements for application development and maintenance process when done in-house. • contractual right to audit development processes and controls shall be ensured. Acceptance testing shall be carried out for the quality and accuracy of the deliverables • Security thresholds shall be used to establish minimum acceptable levels of security and privacy quality;
3.1.2.3	**Correct Processing in Applications**	1. Data input to applications shall be validated to ensure that this data is correct and appropriate. 2. Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts. 3. Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented. 4. Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances 5. Installation of unapproved software and utilities shall be barred by centrally enforced policy 6. Users shall use only organization approved collaboration software
3.1.3	**Availability standards**	1. 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. 2. For all information systems requiring high availability, management shall carry out the following functions: • When an asset is procured, it shall be ensured that the asset configuration provides for fault tolerance. • After procurement, system shall be configured at an availability mode depending on the level of criticality.

		• Develop a plan for availability monitoring, reporting and management. • Optimize availability through monitoring and reporting of equipment performance.
3.2	**Risk Assessment of new technology**	
3.2.1	**Scenarios**	1. Technology Risk assessment shall be carried out for the following scenarios: a) Introduction of new process or technology b) Changes to existing process or technology 2. Technology risk assessment shall be performed by the respective IT or business team responsible for introducing the new process / technology or changes to them. 3. Technology Risk assessment shall be carried out based on technology risk assessment templates and/or checklists defined by the IS team.
3.2.2	**Technology risk assessment Process**	Technology risk assessment shall be performed as per guidelines provided in 'IS Policy - General Guidelines 1.8 Risk Management'
3.2.3	**Architecture and Interdependencies**	1. Technical and functional architecture for any new Information Systems developed / procedure by Organization shall be reviewed and approved by the IS team from an information security perspective 2. Interdependencies of the new information system being developed / procedure shall be assessed with the overall Organization environment from an information security perspective.
3.2.4	**System changes control and procedures**	1. Formal change control procedures shall be documented and enforced to ensure the integrity of system, applications and products, from the early design stages through all subsequent maintenance effort.

		2. Introduction of new systems and major changes to existing systems shall follow a formal process of documentation, specification, testing, quality control and managed implementation. 3. The change control procedures shall include but not be limited to: a) maintaining a record of agreed authorization levels; b) ensuring changes are submitted by authorized users; c) reviewing controls and integrity procedures to ensure that they will not be compromised by the changes; d) identifying all software, information, database entities and hardware that require amendment; e) identifying and checking security critical code to minimize the likelihood of known security weaknesses; f) obtaining formal approval for detailed proposals before work commences; g) ensuring authorized users accept changes prior to implementation; h) ensuring that the system documentation set is updated on the completion of each change and that old documentation is archived or disposed of; i) maintaining a version control for all software updates; j) maintaining an audit trail of all change requests;
3.2.5	**Technical review of applications**	1. Review of application control and integrity procedures shall be performed to ensure that they have not been compromised by the operating platform changes. 2. Ensure that notification of operating platform changes are provided in time to allow appropriate tests and reviews to take place before implementation. 3. Ensuring that appropriate changes are made to the business continuity plan
3.2.6	**System security testing**	1. New and updated systems shall require thorough testing and verification during the development processes, including the preparation of a detailed schedule of activities and test inputs and expected outputs under a range of conditions.

<table>
<tr><td></td><td></td><td>2. For in-house developments, such tests shall be initially performed by the development team. Independent acceptance testing shall then be undertaken (both for in-house and for outsourced developments) to ensure that the system works as expected and only as expected.
3. System acceptance testing shall include testing of information security requirements and adherence to secure system development practices. The testing shall also be conducted on received components and integrated systems.
4. Testing shall be performed in a realistic test environment to ensure that the system does not introduce vulnerabilities to the organization’s environment and that the tests are reliable.
5. The use of operational data containing personally identifiable information or any other confidential information for testing purposes shall be avoided.</td></tr>
<tr><td>3.3</td><td>RACI Matrix</td><td><table><tr><td>Responsible</td><td>Accountable</td><td>Consulted</td><td>Informed</td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td></tr>
</table>

Policy No.:	**2.6**
Policy Name:	**2.6. Information systems maintenance**

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: a. Ensure conformance with all appropriate security requirements b. Protect information assets contained in the information system c. Protect the system against new emerging risks d. Prevent the introduction of new risks when the system is modified e. 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 Organization's desired practices concerning Information Systems Maintenance.
2	**SCOPE**	This policy applies to all information systems where Organization's information assets are stored or processed, and all communication and network connections through which Organization's 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.
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.

3.1	**Backup and Restoration**	1. 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 standard defined by the IS team. Data restoration testing must be performed at a minimum of six months for critical assets or more frequently, as required by the business. 2. 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. REs shall backup data and periodically restore such backed-up data to check its usability. 3. All backup media shall be encrypted. 4. A log of backed data restored from backup media shall be maintained. 5. The number of backup sets to be maintained shall be decided based on the criticality of the information residing in the information systems. 6. 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. 7. All movement of tapes between offsite and onsite locations shall be tracked and recorded. 8. To verify the readability of the backup media, mock restoration tests shall be carried out as defined in the backup and restoration standard, 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. 9. Testing the ability to restore backed-up data shall be performed onto dedicated test media, not by overwriting the original

		media in case the backup or restoration process fails and causes irreparable data damage or loss; 10. The contents of the Web site of Organization shall be backed-up to ensure an orderly recovery, if the site is corrupted 11. Backups shall be reviewed periodically and procedures aligned to minimize downtime impact. 12. Operational procedures shall monitor the execution of backups and address failures of scheduled backups to ensure completeness of backups according to the backup policy. 13. The retention period for essential business information shall be determined, taking into account any requirement for archive copies to be permanently retained.
3.2	**Patch Management**	1. 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. 2. 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. 3. Each patch identified shall be taken through the following process. 4. The patch shall be evaluated for their relevance to Organization, and determine whether it represents a normal or emergency change. 5. A process shall be defined to determine the days within which the identified patches would be fixed. 6. Perimeters shall be defined for classifying patches 7. All patches shall be tested in the Organization operated test environment for feasibility of their application in Organization's production environment. 8. If there is a need for hot fix/priority/critical security patches to be applied to the systems as directed by regulator/ advisories

		/product OEMs, Organization may assess and take necessary approval from CISO and CTO for the exception. 9. 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. 10. 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 Organization's network or enterprise information assets.
3.3	**Job Scheduling**	1. 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. 2. All jobs that are run in the production environment shall be approved by the information system owners. 3. All scheduled jobs shall be monitored for their performance, success/ failure, and the results shall be documented. 4. The results of a scheduled job shall be reviewed within reasonable time and action shall be taken based for any non-standard behaviour including failure of the scheduled job or it part thereof. 5. Schedules shall be subject to change either through planned or emergency requests. 6. The team responsible for maintenance and monitoring of information systems shall be responsible for scheduling and monitoring jobs with respect to the schedule. 7. Any non-standard behaviour including failures shall be raised as incidents and tracked for closure as per the incident management policy. 8. 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.

		9. 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.
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. a) The results and logs of the monitoring activity should be analyzed for occurrence of security incidents and incidents shall be tracked for closure as per the incident management policy. b) 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 Organization meet or exceed the performance targets. c) A capacity plan shall take into account aspects such as normal workloads, special contingencies and storage requirements. d) Insurance companies shall identify trends in usage, particularly in relation to business applications or information systems management tools. e) Thresholds shall be documented and monitored. f) Future capacity requirements shall be projected to ensure that adequate processing power and storage are available. g) System tuning and monitoring shall be applied to ensure and, where necessary, improve the availability and efficiency of systems.
3.5	**Malicious Software Management**	1. Organization shall develop formal and documented procedures for controlling and managing malicious code or malicious software such as viruses, Trojans, worms, logic bombs, etc. The procedures shall also include prevention, detection and recovery controls for malicious codes or malicious softwares. 2. All servers, desktops, workstations, hand-held devices, gateways and any other access points to Organization's network shall be protected against malicious activities (this

		shall include viruses, trojans, malware, adware, spyware and the like). 3. 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. 4. Controls shall be considered to prevent unauthorized software execution. 5. Protection software such as anti-virus, anti-malware, anti-spyware, and anti-adware needs to be installed on information systems controlled / used by Organization and and regular update of malware detection and repair software to scan computers and media as a precautionary control shall be ensured 6. The software shall be capable of being updated on a periodic basis from an authentic source of malicious software information. 7. The software must provide real time protection. 8. 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 9. Regular reviews shall be conducted of the software and data content of systems supporting critical business processes and the presence of any unapproved files or unauthorized amendments shall be formally investigated. 10. Appropriate business continuity plans shall be developed for recovering from malware attacks, including all necessary data and software backup and recovery arrangements 11. Procedures shall be implemented to regularly collect information, such as subscribing to mailing lists or verifying websites giving information about new malware

3.6	**Vulnerability Management**	1. Organization shall identify technical vulnerabilities of information systems and network equipment. Vulnerabilities shall be identified periodically through scanning of the systems. 2. Organization shall define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking and any coordination responsibilities required 3. 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, NCIIPC, IRDAI, etc. 4. Organization should track mapping of cybersecurity notifications and advisories from security bodies like CERT-IN, NCCC, NCIIPC, IRDAI, etc. 5. A timeline shall be defined to react to notifications of potentially relevant technical vulnerabilities 6. Organization's IS Operations team shall assess the risk and impact level of the vulnerabilities and also evaluate actual risk and impact level of a vulnerability striking. Appropriate measures shall be taken to mitigate the associated risks. 7. Client system's vulnerabilities shall be measured and Appropriate measures shall be taken to mitigate the associated risks 8. Organization shall perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively. 9. Red Team results shall be documented using open, machine-readable standards (e.g., SCAP). A scoring method shall be devised for determining the results of Red Team exercises so that results can be compared over time. 10. An audit log shall be kept for all procedures undertaken

		11. The technical vulnerability management process shall be regularly monitored and evaluated in order to ensure its effectiveness and efficiency 12. Technical vulnerability management process shall be aligned with incident management activities, to communicate data on vulnerabilities to the incident response function and provide technical procedures to be carried out should an incident occur
3.7	**IT Service Management**	1. Organization shall have a defined and documented service catalogue for its IT services containing information about the currently available IT services at Organization to provide a single source of consistent information of Organization's agreed IT services to all authorized users. 2. Service levels shall be defined for each information system based on the business requirements. 3. Mechanism shall be established to monitor service levels and analyse 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.
3.7	**Separation of development, testing and operational environments**	1. Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment. 2. Rules for the transfer of software from development to operational status shall be defined and documented. 3. Development and operational software shall run on different systems or computer processors and in different domains or directories. 4. Changes to operational systems and applications shall be tested in a testing or staging environment prior to being applied to operational systems. 5. Compilers, editors and other development tools or system utilities shall not be accessible from operational systems when not required. 6. Sensitive data shall not be copied into the testing system environment unless equivalent controls are provided for the testing system.

<table>
<tr><td></td><td></td><td>7. Users shall use different user profiles for operational and testing systems, and menus should display appropriate identification messages to reduce the risk of error.</td></tr>
<tr><td>3.8</td><td>Control of operational software</td><td>1. Procedures shall be implemented to control the installation of software on operational systems.
2. The updating of the operational software, applications and program libraries shall only be performed by trained administrators upon appropriate management authorization.
3. A configuration control system shall be used to keep control of all implemented software as well as the system documentation.
4. A rollback strategy shall be in place before changes are implemented and an audit log shall be maintained of all updates to operational program libraries.
5. Previous versions of application software shall be retained as a contingency measure and old versions of software shall be archived, together with all required information and parameters, procedures, configuration details and supporting software for as long as the data are retained in archive</td></tr>
<tr><td>3.8</td><td>RACI Matrix</td><td><table><tr><th>Responsible</th><th>Accountable</th><th>Consulted</th><th>Informed</th></tr><tr><td></td><td></td><td></td><td></td></tr></table></td></tr>
</table>

Policy No.:	**2.7**
Policy Name:	**2.7 Mobile security policy**

1	**PURPOSE**	The purpose of this policy is to ensure sensitive and critical data of Organization that is accessible by the employees onto their mobile devices are protected against unauthorized access and prevent unauthorized information disclosure.
2	**SCOPE**	This policy applies to: 1. Employee's personal mobile devices like smartphones and tablet computers that can access Organization's networks, data and systems. 2. Applications used by employees on devices, whether owned by Organization or by employee, which store or access Organization's data. 3. Portable devices such as flash drives, external hard disks, CDs etc.
3	**POLICY**	1. Access to business information shall be provided only after users have signed an end user agreement acknowledging their duties (physical protection, software updating, etc.), waiving ownership of business data, allowing remote wiping of data by the organization in case of theft or loss of the device or when no longer authorized to use the service. This policy shall take account of privacy legislation. 2. The policy also covers separation of private and business use of the devices, including using software to support such separation and protect business data on a private device.
3.1	**Mobile Device Management**	1. Mobile Device Registration- All mobile devices shall be registered and authenticated before being allowed to connect to and access Organization's infrastructure and applications. 2. Device Physical Protection- The user shall be responsible for physical protection of the mobile device. Refer BYOD security policy for BYOD security requirements. 3. Centralized mobile device management- System administrators shall use a centralized mobile device

		management (MDM) solution for the management of all registered mobile devices. 4. User Access Profiles – Access to Organization's resources shall be granted based on business need. 5. Lost / Stolen Devices – When Mobile Devices or Removable Media containing Sensitive Data or Organization's connection information is lost or stolen, a report shall be filed immediately. Refer to section 'Incident Management' in this policy for details. 6. MDM Software Features - The MDM solution shall, at minimum, have the following features: • Deletion (often known as remote wipe) to securely destroy all information stored on the device and any attached storage. • Data Encryption- Mobile devices shall use hardware encryption and deploy file-based encryption software. • Training shall be arranged for personnel using mobile devices to raise their awareness of the additional risks resulting from this way of working and the controls that should be implemented
3.2	**Incident reporting**	1. MDM users shall report immediately to system administrator for data wiping, in case of their device being misplaced or stolen. 2. In case an owner device is hacked for manipulation or deletion of stored data, device owner shall take action and report to the system administrator.
3.3	**Log management**	Detailed logs shall be recorded and managed for MDM.
3.4	**RACI matrix**	**Responsible** | **Accountable** | **Consulted** | **Informed** [illegible]

Policy No.:	2.8
Policy Name:	2.8 Bring your own device (BYOD) policy

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. The purpose of this policy document is to: i) Define employee eligibility for using personal-owned smart phones/tablets to access corporate data ii) Define the responsibilities, guidelines, and terms of use for personal-owned devices. This policy has been defined under the provisions of the Organization 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 Guidelines: Governance' iii) Ownership and interpretation' for further information.
2	**SCOPE**	This policy applies to: • All mobile devices, owned by employees inclusive of smartphones, mobile or cellular phones, PDAs and tablet computers, that have access to Organization's networks, data and system • Applications used by employees on their own personal devices which store or access corporate data • Use of device both during and outside office hours and whether or not use of the device takes place at normal place of work This policy does not apply to laptops.
3	**POLICY**	This document provides policies and rules of behaviour for the use of personally-owned smart phones and/or tablets by Organization employees to access Organization resources and/or services. Access to and continued is granted on condition that each user reads, signs, respects and follows the Organization's policies concerning the use of these resources and/or services. This policy is intended to protect the security and integrity of Organization's data and technology

		infrastructure. Limited expectations in the policy may occur due to variations in the devices and platforms.
3.1	**Eligibility and ownership**	1. All full time employees shall be allowed to configure their personally owned devices for corporate email, application and data access (BYOD program). 2. Contractors or third party employees can enroll their personal devices under BYOD program after due management approvals (on case to case basis).
3.2	**Acceptable devices**	1. Organization'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. 2. Organization shall support devices with OS platforms - a. Android - OS version (N-1) and above b. Apple - iOS version (N-1) and above c. Windows - OS version (N-1) and above The Organization shall ensure the software versions are updated with most current version (N-1) or above. 3. Organization BYOD program does not support personal devices (mobiles/laptops) using customized, "rooted", or "jail broken" versions of operating systems. 4. The device must have a licensed version of the Operating System installed.
3.3	**Device setup**	Organization's IT functions would setup a self-configuration portal for BYOD enrolment. Eligible employees shall be provided access to this portal to setup and configure their devices. Organization's IT function shall support in configuration in case of any issues
3.4	**Ongoing support and device maintenance**	1. Organization's IT functions shall provide support for corporate applications and corporate data on devices enrolled as part of BYOD program. 2. Organization's IT functions would not own the support for managing employee's personal device hardware/ non-corporate software issues.

3.5	**Employee/ Device Exit Process**	1. In case of employee resignation/ exit from Organization– Refer to 'Security Policies: Human Resource Security.' 2. 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 Policies: Incident and Problem Management'. 3. In case of loss of device, the employee shall inform IT function within a defined time. IT function shall perform remote wipe of corporate data from the device as per Annexure 1 as defined below. In case the remote wipe is not possible, the same shall be reported as an Information Security incident as per 'Security Policies: Incident and Problem Management'. 4. Organization shall deploy appropriate information security controls on the devices enrolled under BYOD program to enforce appropriate access controls defined in the 'Security Policies: Access Control.' 5. This may include installation of a Mobile Device Management (MDM) tool.
3.6	**Periodic audit and non-compliance remediation**	IT function will be authorized to monitor or periodically review the device configurations (as per the 'General Guidelines: Acceptable Usage – (II). Acceptable usage of personal devices for official purposes. Point (c)' to identify any exceptions to Organization's policies. The monitoring and logging of activities on the mobile device shall be performed in compliance with 'Security Policies: Monitoring, Logging and Assessment'.
3.7	**Annexure 1**	
3.7.1	**Key definitions**	
3.7.1.1	**Data classification**	1. Corporate Data – means applications and data belonging to Organizationor 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 Policies: Data Classification.' 2. Personal Data – any data/ applications other than Corporate Data, present on the employee's device
3.7.1.2	**Device type**	1. 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. 2. Tablet – is a wireless, portable personal computer with a touch screen interface. The tablet form factor is typically larger than a smart phone. 3. 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.
3.7.2	**Security of personal devices**	The Organization shall configure security controls, such as the following, on personal devices having access to corporate data:
3.7.2.1	**Device security**	1. 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. 2. Access to Organization applications / data: As defined in the 'Security Policies: Access control', access to all Organizationapplication and/or data will be based on two-factor authentication. 3. Device Locking: The device shall be locked after 5 minutes of inactive time. 4. Device Tracking: To determine the location of an employee's handset, devices shall be installed with software to track the same.

		5. Remote Locking: In the case of a lost or stolen phone or tablet, employees or Organization's IT function shall be able to remotely lock or, erase the specified device. 6. 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.
3.7.2.2	**Data security**	1. Remote data wipe: Devices enrolled under this policy shall be configured for remote erase capability through appropriate means such as an MDM software 2. Data encryption and containerization: Please refer to 'Security Policies: Cryptographic Controls.' 3. Application blacklisting: Organization's IT function shall maintain a list of applications that are to be denied system access and shall prevent them from installing or running.
3.8	**Acceptable use**	Refer to 'General Guidelines: Acceptable Usage policy'
3.9	**RACI Matrix**	

Responsible	Accountable	Consulted	Informed

Policy No.:		2.9
Policy Name:		2.9 Change Control
1	PURPOSE	To define consistent and systematic practices for efficient and prompt handling of all changes to Organization's information resources in order to minimize the impact of the changes on information assets.
2	SCOPE	Any change to Organization's information systems 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
3	POLICY	All changes to Organization'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 Organization'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.
3.1	Change Governance	Change governance will be followed as per IT governance framework.

3.2	**Change Classification**	1. All changes shall be classified based on the following factors: 4. Data impacted by the change 5. Impact of the change on Organization's IT environment. 2. 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 IS team. Results of TRA shall be reviewed by the IS team on periodic basis.
3.3	**Change life cycle**	1. Separate environments shall be created and maintained for development and testing of changes to information systems 2. 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. 3. 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. 1. All changes to Organization'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. • Roll Back – All changes should include a rollback procedure for aborting and recovering from failed changes. • 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. 2. 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. 3. All updates to the web site shall be independently reviewed, approved and tested 4. All emergency changes shall however be appropriately documented and post-facto approvals from relevant authorities shall be obtained. When changes are made, an audit log containing all relevant information shall be retained. 5. Document the emergency control procedures to capture the approvals from Head of Operations on an email post any verbal approval being given.

3.4	**Release Management**	1. Releases to both packaged and bespoke applications within Organization shall follow the formal release management process. 2. The release management process of Organization shall have the following considerations: 3. 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. 4. All release related communication shall be sent to the relevant stakeholders well in advance of the release. 5. Appropriate version control procedures shall be followed to ensure the release and its supporting documentation is version controlled. 6. 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.
3.5	**RACI Matrix**	

Responsible	Accountable	Consulted	Informed

Policy No.:	2.10
Policy Name:	2.10 Incident and problem management

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 Organization. Problem Management includes the activities required to diagnose the root cause of incidents and to determine the resolution to those problems. This policy defines Organization's desired practices concerning Incident and Problem Management.
2	**SCOPE**	This policy shall apply to all incidents resulting from violation of Information Security policies or processes / standards defined by the IS 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.
3	**POLICY**	Organizationshall 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.
3.1	**Definitions**	1. **Security/ Operational incident:** A "Security/Operational incident" is an adverse event where: ▪ the IT resource is attacked or threatened with an attack; ▪ accessed/monitored/modified without authorisation; and ▪ used in a manner inconsistent with the established organization's/regulatory policy resulting in a real or possible loss of confidentiality, integrity or availability of the IT resource or information.

		Examples of Security incidents are: ▪ internal or external attempts (either failed or successful) to gain unauthorised access to the IT system or its data; ▪ DLP violations ▪ Attempts (either failed or successful) to gain access to blocked sites as per proxy rules ▪ denial of service (DoS) or unauthorised disruption to IT system and infrastructure; ▪ actual or suspected loss of proprietary, confidential or entrusted information of the organization; ▪ changes to system hardware, firmware or software characteristics without the department head knowledge, instruction or consent; ▪ malicious code (virus, Trojan horse) attacks; ▪ social engineering (tricking someone to disclose confidential/proprietary information like passwords that could compromise system security); ▪ signature update failure; and ▪ hoaxes (deliberate trickery intended to gain an advantage e.g. false virus warnings may lead some user to ignore all virus warning messages, leaving them vulnerable to a genuine, destructive virus). Examples of Operational incidents are: ▪ firewall hardware failure; ▪ anti-virus appliance hardware failure; ▪ IDS hardware failure; and ▪ Any other event as provided under Cert-In directions issued from time to time. **2. Problem/ Event:** An event is an observed or observable occurrence in a system, a network or daily operations. An event will be termed as an incident if it is considered to have "adverse" impact on the IT system/infrastructure or through pre-positioned criteria that describes the circumstances under which events will automatically be deemed adverse. An event will be an incident when it is analysed and classified to be adverse by the incident response team.

		Until events are classified not adverse, they are considered as "suspected incidents". **3. Incident Response Team (IRT)** The Incident Response Team (IRT) is formed to address any incidents and initiate immediate action to resolve the same. The Incident Response Team issues guidelines proactively to address potential threats/ risks arising out of incidents. While incidents shall be handled at various levels based on the severity and impact of the incidents; however, most incidents are to be handled at the Incident Response team leader level. The team shall consist of the following members: ▪ Incident Management Leader (IML): The CRO and COO together play the role of IML at Organization. The Incident Management Coordinator shall keep IML informed about the proceedings of the incidents and the same shall be reported to the Control Management Committee The IML or a person designated by him/her only can officially communicate with the media in case of any incidents. ▪ Incident Management Coordinator (IMC): The CISO and CTO together play the role of IMC at Organization. The IMC shall work with the Incident Response Team Leaders to contain the damage caused by the incident and they shall be the focal point for recovery efforts. ▪ Incident Response Team Leaders (IRTL): BCM Manager shall be the Incident Response Team leader for all Business continuity related incidents. For all issues and incidents related to IT shall be handled by IT Manager. CISO shall be the team leader for all IS related incidents. Non-IT incidents like physical security shall be managed by Admin head. IRTL shall delegate action on incidents to Incident Response Team members. ▪ Incident Response Team Members: The members of the Incident Response Team should get detailed briefing from IRTL before acting on any incident. They should also meet the person reporting the incident for obtaining further

		information. IRTL and IR Team members must have the list of all emergency contact details of the entire Incident Response Team, Vendors, Suppliers, Service providers, etc. An emergency pocket sized card can be prepared containing contact numbers of the Incident Response Team members and distributed to all the employees. ▪ Help Desk Team: It is the responsibility of helpdesk team to: ▪ Answer, evaluate, and prioritize the incoming telephone, e-mail, and in-person requests for assistance from users experiencing problems with hardware, software, networking, security and other computer-related technologies; ▪ Escalate problems to help desk support engineers; ▪ Escalate any security incidents/problem to the IT and system security departments promptly; ▪ Call software and hardware vendors to request service regarding defective products; and ▪ Log and track calls using remedy problem management database and maintains history records/related problem documentations.
3.2	**Reporting IS Event and Weaknesses**	1. 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. 2. 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 Organization's security policies and procedures shall be considered incidents. 3. Incidents shall be reported through the established mechanisms only in reasonable time. 4. 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.

3.3	**Incident recording and classification**	1. 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 2. All incidents shall be classified into High, Medium or Low severity, based on the following criteria as per standards 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 3. All incidents shall be categorized as IS incident, IT incident, Non-IT Incidents. 4. Information security incidents shall be responded to by a nominated point of contact and other relevant persons of the organization or external parties 5. Post-incident analysis shall take place, as necessary, to identify the source of the incident
3.4	**Escalations and Tracking**	1. Appropriate contacts with relevant authorities shall be maintained to escalate to the respective authorities as required. 2. All high, medium and low severity incidents shall be reported to the CISO. 3. Enterprise wide monitoring of Information security incidents shall be done by SOC team on 24X7 basis 4. Continuous monitoring of IT logs to review unauthorized Login/Logout by users, access violations etc. shall be done through Security Information and Event Monitoring (SIEM) and monitored by Security Operations Centre (SOC)

		5. All involved response activities shall be properly logged for later analysis;
3.5	**Management of IS Incidents and Improvement**	1. Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents. 1. Mechanisms shall be established to analyze all incidents in reasonable time and contain the impact of the incidents to the least possible scope. 2. Mechanisms shall be established to resolve all incidents within timelines defined by IS teams for the incident's respective classification. 3. Mechanisms shall be established to recover any loss or damage to information assets as a result of the incident. 4. 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. 5. The CISO should ensure that one or more of the following measures are implemented to identify events that could result in an incident: • Logging and monitoring established on all critical infrastructure information systems • Detective controls such as File Integrity Monitors, MD5 hash implemented on critical files and systems
3.6	**Notification to regulatory authorities**	1. Organization shall identify how incident shall be reported to internal parties and external organizations (e.g. Regulators, media, law enforcement, customers, IRDAI, CERT-In, CSIRT-Fin, Cyber Swachhta Kendra). 2. The timelines prescribed for reporting incidents to external organizations shall be strictly adhered to. 3. Organization shall mandatorily report cyber incidents to Cert-In within 6 hours of noticing or being brought to notice about such incidents with a copy to IRDAI and other concerned regulators / authorities. The details regarding methods and formats of reporting cyber incident is published on Cert-In website.

		Organization shall ensure that contact details of Ministries, stakeholders, vendors and agencies like NCIIPC & CERT-In for incident resolutions are up to date and documented.
3.7	**Root Cause Analysis and Problem Management**	1. 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 2. Internal procedures shall be developed and followed when dealing with evidence for the purposes of disciplinary and legal action. 3. 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. 4. Upon determination of the resolution to identified problems, corrective steps shall be implemented through the appropriate control procedures, especially Change Management processes.
3.8	**Knowledge Management**	1. Mechanisms shall be established to record the resolution and known causes of incidents and problems in a knowledge base. 2. Incident management teams shall be provided access to the knowledge base to reduce the time to respond to incidents. 3. The information gained from the evaluation of information security incidents shall be used to identify recurring or high impact incidents.
3.7	**RACI Matrix**	Responsible | Accountable | Consulted | Informed [ ] | [ ] | [ ] | [ ]

Policy No.:	**2.11**
Policy Name:	**2.11 Network Security**

1	**PURPOSE**	To define Organization's desired security requirements for protection of the IT network used or controlled by Organization.
2	**SCOPE**	1. This policy shall apply to all communication and network connections through which Organization's information assets are transmitted. 2. Communications and network connections include but are not limited to network devices such as routers and firewalls, servers and mainframes. 3. All Business Units or Departments using information technology must comply with these Information Security Policies
3	**POLICY**	1. Networks (connectivity infrastructure and related devices) used for Organization's communication or under Organization's control shall be appropriately secured to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of Organization's information. 2. Organization's 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 Organization's network shall be provided to users only after formal approvals. 3. Network resources belonging to or under control of third parties that has been entrusted to Organization shall be protected in the same manner as Organization's network resources and in accordance with other agreement. Should 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. 4. Any breach of this policy shall be considered as an incident and shall be treated as per the incident management policy.

3.1	**Network Connectivity**	1. Responsibilities and procedures for the management of networking equipment shall be established. 2. Special controls shall be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications. 3. Appropriate logging and monitoring shall be applied to enable recording and detection of actions that may affect, or are relevant to, information security. 4. Systems on the network should be authenticated and systems connection to the network shall be restricted 5. The ability of the network service provider to manage agreed services in a secure way shall be determined and regularly monitored, and the right to audit shall be agreed
3.1.1	**Modes of Connectivity**	1. The modes of connectivity to Organization's 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: • MPLS • Broadband & VPN • Wi-Fi • Wired Network 2. Any network connection allowing access to Organization'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 Organization's policy. 3. Micro segmentation shall be implemented in a network to create separate zones for countering lateral movement and assigning appropriate privileged access as defined in the policy.In case of group companies, infrastructure, networks and databases must be logically and/or physically separated and ensured that IT Personnel having access to group companies are different wherever possible.

		For all administrative tasks or tasks requiring elevated access adequate controls shall be implemented.
3.1.2	**Types of Connectivity**	1. Only trusted entities shall be allowed full access to the Organization's network. 2. All entry points to the Organization's network shall be reviewed and approved. 3. Access to the network shall be via a secure log-on procedure, designed to minimize the opportunity for unauthorized access. 4. All policies within the Access Control Policy shall apply to network connectivity. 5. All connections via corporate computer and communication system shall be protected by authenticating connected users, devices or services. 6. Any connection to Organization's IT Assets classified as business transaction systems and high severity systems from outside Organization-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. 7. Only authorized scripting languages shall run in all web browsers and email clients. 8. Insurance companies shall ensure that only fully supported web browsers and email clients are allowed to execute within the organization, ideally only using the latest version of the browsers and email clients provided by the vendor. 9. Organization shall segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs). 10. Preventive control shall be put in place to block Unauthorized Collaboration tools on the firewall/network security devices.
3.2	**Perimeter Security**	

3.2.1	**Identification of perimeter devices**	1. Organization 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. 2. 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.
3.2.2	**Baseline security standards**	1. Minimum Baseline Security Standards (MBSS) shall be defined for all types of perimeter security devices for all variants (make / model / versions) of the devices. 2. Any changes to the baseline security standards shall be subject to the Change management policy. 3. 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. 4. Baseline security standards shall be reviewed periodically 5. Application whitelisting software shall ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc.) are allowed to load into a system process. 6. Application whitelisting software shall also ensure that only authorized scripts are allowed to run on a system.
3.3	**Network Management**	1. All network equipment and communication lines shall be identified, documented and updated regularly. 2. Network diagrams for local and wide area networks shall be maintained and updated regularly. 3. Security systems operating within and across public and Organization networks shall be protected against internal and external intruders. The systems shall be installed in a physically secured and access-restricted area. 4. The use of personal communications equipment (modems, ISDN cards, data cards, 3G data SIM etc.) attached directly to personal computers with remote control software shall be prohibited.

		5. Access to all communication equipment shall be subject to the access control policy, including the avoidance of generic user accounts. 6. An active discovery tool shall be utilised to identify all sensitive information stored, processed, or transmitted by the Organization's technology systems, including those located on-site or at a remote service provider, and update the sensitive information inventory. 7. Adequate measures shall be taken to isolate and secure the perimeter and connectivity of the servers running monetary transactions applications/process.
3.4	**External Networks**	1. 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. 2. Access to external network resources shall be based on business requirements which shall include adherence to access control procedures. 3. Connecting Organizationmobile assets to unauthorized Wi-Fi access points and Hot spots shall be prohibited. 4. User awareness training shall include acceptable use and cautions, copyright issues and disciplinary action for violation of acceptable use policy and general Internet ethics. 5. Organization shall reserve the right to monitor user actions on public networks, when such networks are accessed through information systems owned or controlled by Organization, in order to protect the confidentiality of Organization's information assets. 6. Organization 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) Organization's network resources. 7. Organization shall protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For

<table>
<tr><td></td><td></td><td>applications that are not web-based, specific application firewalls shall be deployed if such tools are available for the given application type. If the traffic is encrypted, the device shall either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall shall be deployed.
8. Organization shall subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.</td></tr>
<tr><td>3.5</td><td>RACI Matrix</td><td><table><tr><td>Responsible</td><td>Accountable</td><td>Consulted</td><td>Informed</td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td></tr>
</table>

Policy No.:	2.12
Policy Name:	2.12 Cryptographic Controls

1	**PURPOSE**	To define the desired practices for use of cryptographic controls for protection of confidentiality and integrity of Organization's organizational assets.
2	**SCOPE**	1. 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. 2. This policy shall apply to all forms of cryptography applied either to encrypt information in transit or at rest. 3. This policy shall apply to all information systems where Organization's information assets are stored or processed, and all communication and network connections through which Organization's Information Assets are transmitted which utilize cryptography as a mechanism for security of the information asset.
3	**POLICY**	1. Organization shall ensure that appropriate cryptographic controls are applied to data depending upon its classification as per encryption requirements defined in the data classification policy. 2. Any breach of this policy shall be considered as an incident and shall be treated as per the incident management policy.
3.1	**Use of Cryptographic Controls**	1. The management approach towards the use of cryptographic controls across the organization, including the general principles under which business information shall be protected 2. Risk assessment shall be carried out to identify the needs, methodology, business areas and usage of encryption or cryptography. 3. Cryptographic controls shall be used for securing information that is confidential and restricted and transported by mobile or removable media devices or across communication lines; 4. 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. 5. 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 and immutable. 6. 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. 7. The approach to key management, including methods to deal with the protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised or damaged keys shall be defined.
3.2	**Key Management**	1. A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle 2. All cryptographic keys shall be protected against modification and loss 3. 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. 4. The length of the cryptographic keys shall comply with contractual requirements and regulations laid down by competent authorities. 5. 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. 6. Activation and deactivation dates for keys shall be defined so that the keys can only be used for the period of time defined in the associated key management policy. 7. Key management life cycle shall be comprised of the six stages. Each component represents a set of processes that shall be addressed both in documentation and in practice: a. Creation - Key creation shall be conducted in a secure environment (hardened system), and may include the need to conform to requirements for separation of duties. b. Backup - The backup shall imply writing the key to external media (e.g., CD, DVD, USB drive) and storing it in a physical vault.

<table>
<tr><td></td><td></td><td>c. Deployment - 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.
d. Monitoring – Monitoring for unauthorized administrative access to crypto systems shall take place to ensure that unapproved key management operations are not performed.
e. Expiration - The chosen strength of an encryption key shall primarily take into consideration the length of time for which the data may be valid.
f. Destruction - Key destruction shall follow secure deletion procedures so as to ensure that it is properly obliterated.
g. Logging and auditing of key management related activities</td></tr>
<tr><td>3.3</td><td>RACI Matrix</td><td><table><tr><td>Responsible</td><td>Accountable</td><td>Consulted</td><td>Informed</td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td></tr>
</table>

Policy No.:	2.13
Policy Name:	2.13 Business Continuity Management and Disaster Recovery

1	**PURPOSE**	Organization'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, Organization must be able to resume operations in a reasonable time frame without compromising security. This policy defines Organization's desired disaster recovery practice to ensure adequate mitigation of risks from interruption of Information Technology services.
2	**SCOPE**	This policy shall apply to all office locations and systems through which Organization's information assets are stored or processed, and all communication and network connections through which Organization's 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.
3	**POLICY**	All Organization's information systems and assets shall be protected against potential failure or disruption of service through a formal business continuity plan and disaster recovery plan that: • Restores assets in accordance with system or asset criticality to Organization business processes • Maintains the required level of security over Organization'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.
3.1	**IT Availability Management**	
3.1.1	**Capacity monitoring and planning**	Organization 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 Organization.

3.1.2	**System acceptance**	1. 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. 2. 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.
3.2	**IT Continuity Management**	
3.2.1	**Data backup**	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 Organization'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.
3.2.2	**IT Continuity planning**	An IT Continuity plan or disaster recovery plan shall be developed for each Organization or system based on appropriate risk assessment and business requirements and shall be approved by the ISRMC.
3.3	**BCM Framework**	Organization'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: • Enterprise-wide business continuation • Continuation of critical applications • Organization's Data Center Disaster Recovery Plans • Network connection / link

		• Roles and responsibilities of all individuals in the Business Continuity and Disaster Recovery Plans I. Business Impact Analysis • RTO and RPO shall be defined for all applications based on the business requirements. • All dependencies on IT systems by the business functions shall be clearly documented. II. Risk Management and Evaluation • Organization shall ensure that adequate coverage is provided in the identification of threat that may cause disruption to the availability of the IT assets supporting the business operations. • A defined and documented Risk Assessment Methodology shall be used to conduct the Risk Assessment Exercise. • Risk Analysis shall be performed at least on an annual basis. • The acceptable levels of risk shall be defined, documented and approved by the management. • Existing controls shall be assessed for their strength and effectiveness. The mitigation of a risk due to the presence of existing controls shall factor in the control strength and control effectiveness values. • Control assessment may be undertaken on a sampling basis as required. In such cases, the sampling frequency shall be clearly documented. • All risks having a risk rating above the acceptable level of risk shall have risk mitigation plans. These plans shall be approved by the management. • Risk Mitigation plans shall have clearly defined ownership for the action points. • The Risk Mitigation plan shall be reviewed and tracked to closure on a quarterly basis. III. IT DR Strategies

		• The IT DR strategy must ensure minimal data loss during exigencies and enable quick recovery and continuity of critical business operations. • The strategies chosen shall be capable of supporting and integration with the business continuity of Organization. • Strategic options shall be evaluated for the technology components and appropriate strategies shall be defined for recovery and restoration of IT systems as per recovery priority. • External (third party) products and services shall be covered by the strategic options chosen where appropriate. • To prevent the synchronization issue among inter-related applications during disaster, the IT DR plan shall include continuous operation-data mirroring to offsite location and stand-by computing and telecommunication IV. IT DR Recovery Planning • The response and recovery plan shall be concise and accessible to those responsible. • The purpose and scope of each IT DR plan shall be defined, approved and understood. • The plan shall set out prioritized objectives in terms of: ▪ Critical IT services to be recovered. ▪ Time span in which they are recovered. ▪ The situation for invoking plans. ▪ The recovery levels for each critical IT service. • The IT DR Plan shall ensure that configuration of servers, network devices and other products at the DC and DR are identical at all times. • The IT DR plan shall include periodic checks with reference to ensuring data and transaction integrity between DC and DR. • The IT DR plan shall ensure that support infrastructures at DC and DR have no single point of failure and building management and monitoring systems are present to constantly and continuously monitor the resources.

		• The data replication mechanism to be followed in IT DR plan shall ensure RPO compliance for critical applications.
		• Stages of escalation and trigger events (interruption, single point of failure) shall be clearly defined.
		• Specific IT DR Plans shall be documented and approved for each application. IT DR shall provide detailed instructions on the recovery and restoration of IT processes and systems for each application.
		• Technology Recovery Procedures for recovering the IT services shall be developed and coverage shall be given to the following areas:
		  ▪ Detailed procedures to restore the application, databases and the associated hardware at the alternate location, taking into account the changed environment.
		  ▪ Detailed procedures to restore the network accessibility
		  ▪ Procedures for data synchronization and handling of the backlog of information resulting from the disruption.
		  ▪ Changes required from the end user to access the application.
		• IT DR plans shall be reviewed at least on an annual basis.
		
		V. Training and Awareness
		• A formal training program comprising of targeted courses and awareness sessions for the relevant staff shall be developed.
		• A process shall be established for evaluating the training requirements for the staff identified to play a key role in the recovery of the IT systems. Appropriate training programs shall be conducted based on the level of skillset and proficiency determined to enable the person to perform the task.
		• DR Drill shall be performed to ensure adherence to Business Continuity metrics.
		• Alternative site options and resource availability shall be planned as a part of Business Continuity and tested for the same.

		• Periodic Participation of organization in national/ sectoral/ organizational Cyber Security Exercises.
3.3.1	**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 Organization. An Organization liaison with the third party service provider shall supervise execution of the disaster recovery activities in the event of a disruption of service to the Organization.
3.3.2	**IS consideration in BCM**	1. 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. 2. 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 Organization's operations. 3. 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. 4. It shall be ensured that any new application introduced in the IT environment of Organization shall have a documented ITDR processes based on its criticality and shall integrate with the existing recovery processes. It shall also have a business defined RTO and RPO. 5. Any changes made that may have an impact on the developed recovery procedures shall be duly identified as a part of the change control process and shall be approved by the ITDR Manager before implementation.

<table>
<tr><td>3.3.3</td><td>Testing of BCP</td><td>1. The business continuity and DR plans shall be tested at least once annually or when significantly changed to identify incorrect assumptions, oversights, or changes in equipment or personnel. Organizations with mature IT/DR program may also perform unannounced DR drills to test their preparedness.
2. Test results shall be reported to the ISRMC and shall be used to revise the BCP / DRP
3. IT DR testing framework shall include DR drills that represent not only plan shutdown but also real disaster scenarios.
4. All IT DR tests shall be conducted after careful planning to ensure no disruption to the business operations. All risk factors shall be documented and communicated to all affected persons prior to test.</td></tr>
<tr><td>3.3.4</td><td>Review of BCP</td><td>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.</td></tr>
<tr><td>3.4</td><td>RACI Matrix</td><td><table><tr><td>Responsible</td><td>Accountable</td><td>Consulted</td><td>Informed</td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td></tr>
</table>

Policy No.:	2.14
Policy Name:	2.14 Third party service providers

1	PURPOSE	To define desired practices concerning the selection, enrolment, and termination of third parties and operations handled by them.
2	SCOPE	1. This policy is applicable to all third party service providers such as contractors, vendors and consultants who handle, store or transmit Organization's information and information resources in any form. 2. 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 Organization information assets are transmitted, stored or processed. 3. 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. 4. All Business Units or Departments utilizing the services of a third party for business operations shall comply with this policy.
3	POLICY	1. All contracts with Third Party service providers shall require that the third-party service providers provide controls to comply with provisions of the Information security policy for Organization information assets accessible to them, 2. This shall be deemed to conclude that the third party shall provide security at a level at least as secure as Organization 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 Organization 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 Organization before access to Organization information assets can be granted. 3. Any breach of this policy shall be considered as an incident and shall be treated as per the incident management policy.
3.1	**Vendor IS classification**	1. All third party service providers shall be classified with respect to Information Security based on a third party service provider classification standard defined by the IS 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 including access to the sensitive information. • Access to non-information assets including Organization premises • Criticality of operations of the third party • Access to Organization's Intellectual property • Providing services having a regulatory significance • Exclusivity and availability of multiple service providers in that line of service or geography 2. The third party service providers' classification standard 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.
3.2	**IS provisions in contracts and SLAs**	1. All third party service providers shall be empaneled for the services of Organization only after a contract is signed between Organization and the service provider. 2. The contracted terms and condition shall be drafted by the Legal department of Organization for safeguarding the interest of Organization in consultation with Compliance, Risk and IS departments. 3. All agreements/documents with third parties shall be digitally signed using a special tool

		4. 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 standard. 5. 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 standard. 6. In order to be able to enforce performance, information security and other controls to address outsourcing risks, Organization shall build the right to audit as part of contract with vendors. Further, based on the access to sensitive and critical data and criticality of operation, the audit and reporting mechanism including the periodicity of the audit may be provided by the Organization. 7. If the vendor is certified under the ISO27001 standard, and if the scope of services provided to Organization is included under the scope / statement of applicability for the certification, the vendor may be accepted from the requirement for periodic audits by Organization. However, in such a scenario, the vendor will be required to furnish the following: 8. a self-certificate of compliance to all IS provisions in the contract 9. Copy of a valid ISO27001 certification demonstrating that the scope of services provided to Organization is included under the scope / statement of applicability for the certification 10. Where vendor providing services to group companies, it shall be ensured that IT personnel with cross-entity access should be segregated, wherever possible, to avoid the risk of one company's data being stored on another company's infrastructure. 11. To ensure oversight of extended supply chains and mitigate third-party cyber risks, Regulated Entities to insist through SLAs that service providers/outsourced entities cannot further outsource activities unless they obtain prior written permission from RE after disclosing details of such further outsourcing if any.

3.3	**Enrolment and change**	1. 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 standard through either the following means: • Self-appraisal by the vendor; • On-site visit by Organization personnel • Information collected from other public sources. 2. 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; • 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 3. 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. 4. Appropriate Due diligence shall be performed to verify sub-contracting arrangements of third party vendors
3.4	**Periodic assessment**	1. 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 organization , as per the periodicity defined in the third party service provider standard. 2. The periodic assessment shall cover:

		• Services mentioned as part contract are performed as per SLA; • Personnel employed by service providers: • are competent with knowledge of product and processes handled • 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 Confidentiality and non-disclosure agreements as defined in the contract 3. The third party shall provide all support in compliance of the Information & Cyber Security Audit observations within the timelines of compliance stipulated in organization's policy.
3.5	**Termination**	1. Organization shall reserve the right to terminate the services of any third party service provider on non-performance or non-conformity to any of Organization's contractual requirements including information security requirements. The clauses for termination shall be clearly laid out in the contract with the service provider. 2. 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: 3. The service provider shall be expected to return any assets that belong to Organization which are in the possession of the service provider during its tenure of service. 4. Access to Organization'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 Organization's information systems / premises.

<table>
<tr><td>3.6</td><td>Data Sharing and retention</td><td>1. Valid business purpose must be defined for the data that needs to be shared with the Third Party Service Provider.
2. Any data generated by the third party in the course of its operations performed for Organization shall belong to Organization and shall follow Organization’s policies.
3. Organization 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.
4. Organization shall have the right to delete organization related information from the vendor assets used for the activity, and certify it as per the data retention policy.
5. Upon the termination of the contract all data transferred by Organization or generated by the third party for Organization, shall be handed-over to Organization.
6. 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.
7. Data will not be shared by the third party with any other entity apart from Organization without explicit approval from Organization and without an explicit contract which mandates compliance with Organization policies.</td></tr>
<tr><td>3.6</td><td>RACI Matrix</td><td><table><tr><td>Responsible</td><td>Accountable</td><td>Consulted</td><td>Informed</td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td></tr>
</table>

Policy No.:	2.15
Policy Name:	**2.15 Physical and environmental security**

1	**PURPOSE**	To define the desired practices concerning physical and environmental security at Organization for ensuring a secure environment for its employees as well as its tangible and intangible assets. The physical security policy of Organization shall aim at ensuring a secure environment for its employees as well as its tangible and intangible assets.
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 Organization i.e. • People such as employees, contractors, service providers / visitors accessing the Organization facilities. • Infrastructure such as building premises, furniture and fixtures, office equipment, physical documents and other electro-mechanical installations
3	**POLICY**	All assets of Organization (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.
3.1	**Zoning and Perimeter Definition**	Facilities of Organization 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:

3.1.1	**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.
3.1.2	**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.
3.1.3	**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: • A special team within Organization • External service providers required to access the Secured Zone for business purposes • Some of the areas within Zone 3 would include: • Dealing Room/ Trading Floor • Operating areas where cash and valuables are kept • Compactor rooms
3.1.4	**Zone 4 or Electronically Sensitive Zone**	1. Zone 4 shall be a demarcated electronically sensitive zone containing electronic assets which may host Organization'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: • A special team within Organization • External service providers required to access the Secured Zone for business purposes • Areas within Zone 4 would include: • Server rooms • Datacenters

		2. Organization 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. 3. Each Secured Zone shall have a designated owner. The Secured Zone owner shall be responsible for • Identifying the persons (internal staff and outside contractor, suppliers and visitors) authorized to access the Secured Zone • Validating the list of persons authorized to enter the Secured Zone on a periodic basis • Revoking all unnecessary / unauthorized access rights to the Secured Zones 4. 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 CISO for taking actions as mandated by the procedure followed at the particular site. In case there is no procedure defined, the CISO 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.
3.2	**Physical Access Standards for Zones**	
3.2.1	**ZONE 1**	1. Building / Premises (referred to as 'Premises' henceforth) shall refer to areas under the direct management control of Organization management as defined below: • In case the entire structure is owned or leased by Organization 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 Organization. • In case where Organization 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. Organization shall request the premises authority to comply with its policies to the extent possible to ensure safety of its own assets. 2. 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 Organization entity (clients). 3. 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: • Lobby / Reception • Meeting rooms in the entrance lobby • Cafeteria if it is outside the perimeter requiring access badges for entry / exit 4. Access to Zone 1 shall be protected from unauthorized access by safeguards such as security guards stationed at entry / exit gates of the Premises. 5. 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 Organization 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. 6. Certain individuals notified by Organization Management can also be restricted from accessing the Premises open to general public. Such a restriction shall need to be notified by the CISO and the in-charge of Premises for each building and shall need to be approved by ISRMC. 7. For Employees / and Long Term Contractors: • All employees of Organization 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. 8. 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.
3.2.2	**ZONE 2**	1. 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. 2. Access to these areas shall be granted to individuals only for professional reasons and only once they have been duly identified. 3. 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. 4. 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. 5. 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. a) For Employees / Long Term Contractors

		I. All employees of Organization 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. II. 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. III. 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. IV. The badge holder shall be responsible for: • Using the badge to gain access to the controlled/secured zone • Wearing the badge noticeably • Not entrusting the badge to another person • Not using the badge to allow access to any other person (tailgating) • Surrendering the badge on expiry of the rights justifying its possession. b) For Service Providers / Entities Authorized to Enter for A Limited Period I. 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. II. Entities authorized to enter the premises for a limited period shall be issued visitor badges with 'V' marked on them.

		III. 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. IV. 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. c) For Visitors Authorized to Enter the Premises On a One-Time Basis 1. 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 Organization 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. 2. The responsibilities of the visitor shall include: a) Wearing the badge noticeably b) Not moving around in the Organization'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 3. 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 Organization's buildings d) Informing his/her visitors of the Organization's rules relating to moving around in the premises e) Ensuring that his/her visitors surrender their badges when the visit is over.
3.2.3	**SENSITIVE AREAS (ZONE 3 AND 4)**	1. 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. 2. 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. 3. Access to these areas shall be granted for strictly professional reasons. Visitors shall not have access to these areas unless required for business purposes 4. 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. 5. 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.
3.3	**Environmental Standards for Zones**	1. Environmental security controls shall be implemented by Organization 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.

		2. The administration teams shall be responsible for the design and implementation of environmental controls and the CISO shall be responsible to ensure their adherence and compliance.
3.3.1	**Zone 1**	1. Buildings shall have minimal points of entry to avoid unauthorized personnel gaining access to building 2. 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 should be provided next to it in Breakable Glass box, which can be used by the employees for opening the door in emergency situation. 3. Buildings shall have appropriate lightning protection which shall be tested on periodic basis 4. 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. 5. 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.
3.3.2	**Zone 2**	1. Work Areas shall be accessed through access control cards to restrict unauthorized entry of any personnel. 2. Work areas shall be monitored for any leakage or any water intrusion. 3. Work areas temperature shall be monitored by the monitoring staff and administered by a person in charge. 4. Work areas shall have sufficient number of fire exit points and employees shall be given training of fire evacuation procedure in case of emergency. Evacuation drills shall be performed at least on an annual basis.

		5. 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. 6. Work areas shall have smoke detectors positioned all over to detect any instance of fire and give warning alarm immediately. 7. Floor plans shall be displayed at specific locations on each floor. 8. Employees are expected not to carry inflammable items.
3.3.3	**Environmental Security For Sensitive Areas (Zone 3 And Zone 4)**	1. Sensitive areas shall be protected from any water leakage and will be monitored by the BMS team. 2. Smoke detectors shall be positioned to detect any instance of fire. 3. 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 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. 4. Sensitive areas (Data Centers, Server Rooms) shall have appropriate fire prevention equipment installed. Preference shall be given to automated fire detection and suppression equipment. Sensitive areas shall have fire-resistant doors, walls to safeguard against fire damage. 5. Temperature for sensitive areas shall be monitored more frequently. Sensitive areas shall have proper electricity backup. 6. Precision air-conditioning systems to support information systems and equipment like server rooms, network rooms, and disaster recovery sites shall be in place. 7. Dual power supply controls to ensure continuous power supply shall be implemented.

<table>
<tr><td>3.4</td><td>Security in Transit</td><td>Appropriate measures shall be implemented by Organization to enable secure transit of information assets stored in Zone 3 or 4.
Organization 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 Organization.
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.</td></tr>
<tr><td>3.5</td><td>RACI Matrix</td><td><table><tr><td>Responsible</td><td>Accountable</td><td>Consulted</td><td>Informed</td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td></tr>
</table>

Policy No.:	2.16
Policy Name:	2.16 Monitoring, Logging and Assessment

1	**PURPOSE**	To define the Organization desired practices regarding monitoring, auditing and assessment of logs.
2	**SCOPE**	This policy applies to all information systems information assets and all communication and network connections through which Organization 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.
3	**POLICY**	All critical information systems deployed by Organization 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. Any breach of this policy shall be considered as an incident and shall be treated as per the incident management policy.

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.
3.2	**Information systems logging and monitoring**	1. All information systems will be configured to log system activities and generate alerts for any unusual activity to system administrators. 2. The activities of privileged users such as system administrators and system operators shall be logged and independently reviewed on a regular basis. 3. Mechanisms shall be put in place to detect and report activity which violates the information security policy with respect to access, acceptable usage and / or any other aspect addressed by the policy. 4. 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. 5. The clocks of all relevant information processing systems within Organization or security domain shall be synchronized with an agreed accurate time source. 6. External and internal requirements for time representation, synchronization and accuracy shall be documented. 7. A standard reference time for use within the organization shall be defined. 8. 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. 9. Where the action to be taken requires changes to the information system configurations, such changes shall be subject to the change management policy. 10. The activity logs and audit trails shall be stored/retained based on the record retention requirements and applicable regulatory compliance requirements. 11. Logging facilities and log information shall be protected against tampering and unauthorized access. 12. Logs shall be made available to the Law Enforcement Agencies, IRDAI, Cert-In and CSIRT-Fin as and when required. 13. ICT infrastructure logs shall be maintained as per regulatory guidelines 14. ICT infrastructure logs shall be maintained for a rolling period of 180 days and within the Indian jurisdiction as per directions issued by Cert-In from time to time. 15. Monitor attempts to access deactivated accounts through audit logging. 16. System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.
3.2.1	**Network access and activity**	1. 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. 2. Mechanisms such as internet access filters shall be set up for adherence to acceptable usage policy of Organization with respect to access to external networks; and the same shall be monitored and reviewed.

3.2.2	**Application access & activity**	User activities, exceptions, and security events on all applications shall be logged and monitored. Logs must include the following: 1. System starting and finishing times. 2. System errors or Faults and corrective action taken. 3. Confirmation of the correct handling of critical data files and computer output. 4. The name of the person/process / system making the log entry. 5. Source address from where data or system is being accessed (this might be either IP address or MAC ID). 6. Application shall prohibit users from logging into the application on more than one workstation at the same time with the same user ID. 7. Secondary Network Connectivity and IT infrastructure shall be provisioned and tested for the critical applications and services.
3.3	**Transfer and Movement of assets**	Organization shall either transfer assets from one Organization entity to the other or move them in and out of Organization facilities when either being procured or sent for destruction. Procedures shall be developed for entry /exit to and from Organization premise regarding new assets which have been procured or assets which are sent to the vendor premises for repair / sent for destruction / sale
3.4	**User activity monitoring**	1. User accounts shall be monitored regularly to detect any unwanted privileges, orphan accounts, and dormant accounts. Any accounts detected in violation of Organization's policies shall be suspended or terminated. 2. Redundant/dormant user IDs shall not be issued to other users. A periodic account review shall be conducted and respective managers shall be required to match the current user rights with the business requirements.
3.5	**Information Security assessment**	

3.5.1	**Security assessments for infrastructure and applications**	1. The IS team will define standards for conducting Vulnerability assessments and security review of infrastructure. The standards shall include: a) Frequency of conducting assessments based on criticality of applications within the broader limits provided under this para. b) Coverage of security assessments 2. Continuous Exposure Management (CEM) (internal vs. external) for conducting security assessments based on criticality of applications. VAPT of critical internal applications or infrastructure components to be conducted periodically at least once in a year by a CERT-In empaneled Auditor. 3. VA should be conducted for all internet facing information assets and systems at least once every 6 months by a CERT-In empaneled Auditor. External Grey/White box Penetration Testing (PT) should be conducted for all internet facing information assets and systems once in 6 months by a CERT-In empaneled Auditor. 4. In cases wherein due to unavoidable circumstances the PT is conducted in test environment, the organization shall ensure that the version and configuration of the test environment resembles the production environment for VAPT .Any deviation, shall be placed before ISRMC for approval. 5. Mandatory security testing shall be conducted for all changes to internet facing information assets or systems and reported gaps should be closed before moving into production. 6. Business applications including APIs or Web Services etc. shall undergo Security Audit and VAPT Testing including secure code review before go live and periodically as a part of mandatory Grey/White box VAPT. 7. 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. 8. The results of the assessment report shall be analyzed and acted upon by the team responsible for maintaining required the information system.

		9. High risk gaps, reported from the VAPT, should be remediated immediately, and in no case should go beyond 30 days followed by mandatory re-validation testing. 10. Priority for closure of audit gaps should be based on the risk associated with each gap; however, the outer time limit for closure of all the audit gaps is two months followed by mandatory re-validation testing. 11. All security assessments report and the actions taken shall be reviewed by the Information security team. 12. 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. 13. The procedure for acceptance of risk for the IS Audit observations shall be defined. 14. The results of the assessment shall be communicated to vendors/third party service providers. 15. All vulnerabilities identified through the Responsible Disclosure Framework shall be promptly addressed and closed.
3.5.2	**Internal IS assessment by IS Team**	1. Organization 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 standards defined by the IS team. 2. 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.
3.5.3	**External IS assessment**	1. Organization 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 Information Security team. 2. Formal procedures shall be developed by the Information Security team for planning and reporting audits and audit findings and

<table>
<tr><td></td><td></td><td>ensuring the implementation of a prompt and accurate remedial action.
3. The Information Security team shall be responsible for defining the scope of the review and coordinating with the business and support teams.
4. Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.
5. Independent assurance auditor shall be rotated every three years.</td></tr>
<tr><td>3.6</td><td>RACI Matrix</td><td><table><tr><td>Responsible</td><td>Accountable</td><td>Consulted</td><td>Informed</td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td></tr>
</table>

Policy No.:	2.17
Policy Name:	2.17 Legal and Regulatory Compliance

1	**PURPOSE**	1. To ensure compliance with all relevant legislation and laws (criminal and civil), regulations, standards/guidelines and codes; simultaneously fulfilling the requirements for statutory, regulatory and contractual obligations. 2. To avoid breaches of legal, regulatory, statutory or contractual obligations impacting information security and of any security requirements. 3. This policy requires Organization to ensure that employees and third parties (including vendors & contractors) understand and adhere to legal, statutory, regulatory, contractual, and security requirements that may have an impact on the business.
2	**SCOPE**	The policy applies to all areas and all activities of Organization. Every employee, contractor, sub-contractor, agent and supplier of Organization is required to comply with all aspects of the law and to act ethically, at all times: In this policy, a reference to the law includes: • Acts, regulations, codes, and other subordinate legislations; • Operating licenses and other authorizations; • Government and industry guidelines and practice statements; • Conditions imposed on approvals and other licenses; • Any new relevant guidelines issued in the future
3	**POLICY**	Organization is committed to complying with laws as they apply to it and to demonstrating ethical behavior. Organization will: • comply with all relevant legislation, laws, standards, codes, and internal policies; • monitor compliance with its legal and ethical obligations; and • take appropriate corrective action to prevent recurrence of compliance failures

3.1	**Legal and Regulatory Requirements**	1. All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date. (Please refer Annexure A) 2. Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products. 3. Regulations backed by statute shall be made compulsory. 4. Formal risk analysis shall be done that will enable controls to be selected from policy that address the applicable controls that are required by the principal regulators and legal obligations. 5. It shall be ensured that the local legislative, regulatory and contractual control requirements are identified and included in the list of all Identified legal, regulatory and contractual requirements. 6. Advice and approval on the statutory, regulatory and contractual requirements of Organization Office shall be sought from the legal department. The CISO shall document the requirements in a register with the corresponding controls associated with each regulatory and legal requirement. 7. The legal department shall instruct the employees on the legal requirements and the compliance to such legal requirements. The legal department shall also ensure that the controls are implemented immediately to ensure compliance. Regular review to the compliance shall be carried out by the legal department
3.2	**Adherence to IRDAI guidelines**	1. Circulars / Guidelines are issued by IRDAI stating the amendments in security requirement / working procedure. Organization shall adhere to all applicable guidelines issued by IRDAI. 2. Guidelines issued by IRDAI shall be incorporated in the operation of Organization

<table>
<tr><td>3.3</td><td>Adherence to IT Act ,2000 and Rules, IT (Amendment) Act2008 & Other applicable Acts</td><td>1. Organization shall take preventive steps to protect the confidentiality of customers' data / information as per the act. Amendments have been done in IT Act 2000, latest amendments have been incorporated in it, Organization shall adhere to the guidelines stated in IT Act 2008.
2. The issues relating to e-mail messages, Internet Banking and Communication network in the light of IT Act 2000 shall be adequately addressed.
3. The provisions in the IT Act 2000 shall be clearly understood to protect the data environment in Organization and for prevention of frauds.
4. Procedures shall be devised to comply with amendments to IT Act, 2000 or enactment of supporting Cyber laws or Privacy laws
5. Organization shall adhere to the applicable guidelines stated in the Aadhaar Act guidelines, rules, acts and amendments thereto</td></tr>
<tr><td>3.4</td><td>RACI Matrix</td><td><table><tr><td>Responsible</td><td>Accountable</td><td>Consulted</td><td>Informed</td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td></tr>
</table>

Policy No.:	2.18
Policy Name:	2.18 Situational Awareness

1	**PURPOSE**	Situational awareness refers to the Organization's understanding of its cyber threat environment and the adequacy of its cyber risk mitigation measures.
2	**SCOPE**	This policy applies to Organization' s cyber security controls which is already in place or planned to be implemented in order to mitigate the evolving cyber risks
3	**POLICY**	Organization shall establish and follow a cyber-threat intelligence process, analysis and information sharing process including but not limited:
3.1	**Identification of Potential Cyber Threats**	1. The following Cyber threats shall be identified: • That could affect the operational performance • Cause significant impact to meet Organization's objectives and obligations • Cause threat to critical business, processes and reputation
3.2	**Threat Intelligence Process**	Organization shall establish a process to gather and analyze cyber threat information in conjunction with internal and external business and system information sources
3.3	**Information Sharing**	1. A plan shall be defined for information-sharing through trusted channels when an incident occurs as part of organization's response programs for cyber-attack 2. Organization shall actively participate in information-sharing groups to receive and share indicators relating to cyber incidents. 3. Information sharing arrangements shall be documented in Cyber Crisis Management Plan (CCMP) in case of a large incident to facilitate sector-wide response. Cert-In / NCIIPC guidelines may be used for preparing Cyber Crisis Management Plan including information sharing arrangements.
3.4	**RACI Matrix**	

Responsible	Accountable	Consulted	Informed

Policy No.:	**2.19**
Policy Name:	**2.19 Cloud Security Policy**

1	**PURPOSE**	To define the Organization desired practices regarding Cloud Security.
2	**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. a. Data b. Application c. Functions d. Process e. Network connections f. Underlying Hardware The assets are to be evaluated on the following factors: I. Determine how important the data or function is to Organization II. Analyze the impact of the scenarios: a. The asset becoming widely public and widely distributed b. An employee of the Cloud service provider accessing the asset c. The process or function being manipulated by an outsider d. The process or function failing to provide expected results e. The information/data being unexpectedly changed f. The asset being unavailable for a period of time

3	**POLICY**	The objectives of this policy are: 1. To ensure that the cloud service is in accordance with the business and security requirements and relevant laws and regulations for: 2. Provisioning and Commissioning of Cloud Services. 3. Operations and Management of Cloud Services. 4. De-commissioning of Cloud Services. 5. To evaluate the following factors in cloud adoption decisions: a. 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. b. Risk including availability requirements, regulatory, compliance and statutory requirements, data sensitivity. c. Control over intrusion decisions, vulnerability monitoring, denial of service attacks. Any deviation from this policy shall be treated through risk management and exception management as defined in the ICSP
3.1	**Cloud Service Models**	Cloud service delivery is divided among Four archetypal models **Cloud Software as a Service (SaaS)** 1. The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. 2. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). 3. 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)** 1. 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. 2. 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)** 1. 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. 2. 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)** 1. The capability provided which includes, business process outsourcing (BPO) services that are sourced from the cloud and constructed for multitenancy 2. The Services are often automated, and where human process actors are required, there is no overtly dedicated labor pool per client
3.2	**Cloud Deployment Models**	1. **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 2. **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. 3. **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).
3.3	**Compliance**	Organization shall ensure compliance with various IRDAI guideline and related laws, regulations and guidelines issued by the regulating authority in India as applicable
3.4	**Cloud security lifecycle**	Governance and risk management, while the deployment model may define accountability and expectations. Organization shall ensure before signing an agreement with the cloud service provider, to the complete approval of all the mandatory controls.
3.4.1	**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 3.2.2.3 – 'Authorization Inventory'". Organization shall affirm that the cloud service providers authentication process, access control, accountability and logging is in line with applicable regulatory and legal requirements. Customer data shall be protected from any unauthorized access.
3.4.2	**Physical Security Controls**	The Physical Security Controls shall be followed according to the existing "Information and Cyber Security Policy, Security Domain Policy, Section 2.15 – 'Physical and Environment Security'". The additional physical security controls are mentioned as follows: a. Organization 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. b. It shall be recommended to opt for Cloud service providers that conform to the ISO 27001 standard for physical and environmental security.
3.4.3	**Infrastructure Security (for private cloud and IaaS for public cloud)**	1. Design of the Cloud environment shall be based on appropriate security guidelines such 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. 2. 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. 3. 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. 4. Infrastructure integration architecture shall be defined for integration within the data center and across multiple data center. 5. 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 Organization'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.
3.4.4	**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 2.11. 'Network Security'". Also, Organization shall ensure that the cloud service provider has documented and tested processes for: a. Access controls, for management of the network infrastructure b. Traffic filtering provided by firewalls c. Creating secure Virtual Private Networks (if VPN is offered) d. Intrusion detection / prevention e. Mitigating the effects of DDoS (Distributed Denial of Service) attacks f. Logging and notification, so that systematic attacks can be reviewed.
3.4.5	**Data Isolation**	In case of utilization of cloud services, Organization shall ensure that its data is adequately isolated in the cloud environment. Organization'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: a. 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. b. 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.
3.4.6	**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'".
3.4.7	**Encryption**	1. As defined in the existing "Information and Cyber Security Policy, Security Domain policy, Section2.12 – 'Cryptographic Controls'", Organization shall ensure that appropriate cryptographic controls are applied to data depending upon its classification as per encryption requirements defined in the data classification policy. 2. Organization 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 2.12 – 'Cryptographic Controls". 3. Organization 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. 4. Organization shall prefer Hardware encryption keys, in compliance with the Federated Information Processing Standard (FIPS) 140 2-3 and above, whenever compatible. 5. Organization shall devise encryption, key management procedures in accordance with the already existing Organization's information security policy for the following: a. To encrypt data in transit, at rest, backup media b. To Secure key store

		c. To protect encryption keys d. To ensure encryption is based on industry/ government standards e. To Limit access to key stores f. Key backup and recoverability g. To test these procedures
3.4.8	**Application Security**	Organization 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 – 'Application Security'".
3.4.9	**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 2.10 - 'Incident and Problem Management'".
3.4.10	**Business Continuity and Disaster Recovery**	1. Organization shall ensure Business Continuity for cloud services shall be in accordance with the existing "Information and Cyber Security Policy, Security Domain Policy, Section 2.13 – 'Business Continuity Management and Disaster Recovery'". 2. In addition, Organization shall also audit the Cloud service provider's disaster recovery plan and ensure it meets Organization's requirements. At minimum, the following shall be considered: a. The ability to retrieve and restore data following data loss incidents. b. The cloud service provider shall provide Organizational disaster recovery testing report that would be extensive, covering from exercise scope to the final outcome and recommendations. c. Make sure the DR (Disaster Recovery) solution is capable of maintaining the same levels of security measures and controls utilized in normal operation mode. d. Assure that the Disaster recovery solution is owned and managed completely by the contracted Cloud Service Provider.

		3. It is recommended to opt for cloud service providers who are BS25999 or ISO 22301 certified. 4. Business Continuity Plans shall be in place for cloud sourced services based on regular BCP and provisions for the same shall be included in Organization contracts. 5. A confidential document containing account information for business continuity purposes shall be maintained
3.4.11	**Exception Management**	1. An "exception" shall be defined as circumstances when a particular policy or standard; security program requirement; or security best practice cannot be fully implemented. 2. Organization 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. 3. The Exception Management for Cloud Services shall be followed in accordance with the existing "Information and Cyber Security Policy, General Guidelines, Section 1.8 –'Exceptions'".
3.5	**Off boarding of cloud service provider**	1. Upon termination of contract, all data transferred by Organization, or generated by the third party for Organization, shall be handed over to Organization. Evidence shall be provided to Organization for deletion and purging of all copies of data at service provider site/s 2. 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'. 3. 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 Organization employees.
3.6	**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".

3.6.1	**Evaluation of Cloud Service Provider virtualization environment**	Organization 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: a. Disable or remove all unnecessary interfaces, ports, devices and services; b. Securely configure all virtual network interfaces and storage areas; c. Establish limits on VM resource usage; d. Ensure all operating systems and applications running inside the virtual machine are hardened; e. Validate the integrity of the cryptographic key- management operations; Harden individual VM virtual hardware and containers;
3.6.2	**Virtualization Security**	1. Organization 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 incompliance with the production virtualization environment. 2. Organization shall assure the following controls are applied as a part of hypervisor security: a. Organization can access the Hypervisor administrative access log reports. b. Hypervisor complete logging is enabled. 3. Organization 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. 4. The cloud service provider shall provide Organization with its complete vendor list that will have access to Organization's data; at any point throughout the duration of the agreement. The Cloud Service Provider shall update Organization about any change in the vendor list. 5. For multi-tenancy through virtualization, a. 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. b. 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. c. 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 Organization. Also, using different disk partitions to isolate VMs belonging to different Organizations can provide further isolation.
3.7	**Legal, Regulatory and Contractual Requirements**	
3.7.1	**Contractual Requirements**	1. Organization 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. 2. The cloud services shall be taken only from the Ministry of Electronics and Information Technology (MeitY) empaneled CSPs. The CSP's data center should hold a valid STQC (or any other equivalent agency appointed by Government of India) audit status. **3.** 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. 4. Organization shall prepare a service contract addressing the following domains:

		a. Architectural Framework b. Governance, Risk Management c. Clarity on Cloud service provider's role and Organization's role d. e-Discovery searches e. Expert testimony f. Primary and secondary(logs) data g. Location of storage h. Contract termination i. Ownership of data 5. Organization 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 Organization. 6. Organization shall include the financial remedies in the event of a business disruption in the SLA. 7. Third party service providers shall be empaneled for the cloud services of Organization only after a contract is signed between Organization and the service provider. 8. The contracted terms and condition shall be approved and drafted by the Legal department of Organization for safeguarding the interest of Organization in consultation with Compliance, Risk and Information Security departments. 9. Automated tools shall monitor and track SLA's and generate reports to project the impact on costs, ROI etc. 10. The provisioning process shall be completely automated.
5.7.2	**Contractual clauses on Data Privacy**	1. Organization 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. Organization shall ensure that the cloud service providers are not permitted to use Organization's' data for advertising or any other non-authorized secondary purpose Organization shall contractually assure that they are informed of any confirmed

<table>
<tr><td></td><td></td><td>breach immediately without any delay. For suspected breach, Organization shall be informed within 4 hours from the time of breach discovery.
2. Organization shall contractually require that the cloud service provider will completely eliminate any trace of data/ information in disks, backups, etc., at the termination of the Contract as agreed in the contract.
3. Organization shall contractually require and ensure that the cloud service provider will fulfill the data and media destruction and sanitization controls.
4. Organization shall ensure that the cloud service provider complies with the requirement of return of data to Organization. There shall be no Vendor-lock in by the cloud service provider.</td></tr>
<tr><td>5.7.3</td><td>Regulator Independence</td><td>Organization 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 Organization, though the resources are not physically located in the premises of Organization.</td></tr>
<tr><td>5.8</td><td>RACI Matrix</td><td><table><tr><td>Responsible</td><td>Accountable</td><td>Consulted</td><td>Informed</td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td></tr>
</table>

Policy No.:	2.20
Policy Name:	2.20 Cyber Resilience

1	**PURPOSE**	1. 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. 2. To provide guidelines for addressing cyber security and related risks and the mitigation of such risks.
2	**Scope**	This policy applies to information systems, including IT applications, IT infrastructure and physical information channels, information assets that Organization uses, business processes and procedures.
3	**Policy**	The objectives of this policy are to: 1. Prevent occurrence and recurrence of cyber incidents by implementing security proactive measures. 2. Create infrastructure for conformity assessment and certification of compliance to cyber security best practices, standards and guidelines 3. Create mechanisms for security threat early warning, vulnerability management and response to security threats 4. 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. 5. Promote and launch a comprehensive awareness program on security of cyberspace.
3.1	**Classification**	1. Critical Systems and Cyber Security Incidents shall be classified based on criticality and severity 2. Incident classification guideline shall be defined as a part of Incident Management Procedure for Information & Cyber Security Incidents

3.2	**Cyber Resilience program**	1. 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. 2. 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 protection procedures, consistent control of removable media usage, monitoring of mobile and home working procedures, and ongoing awareness and educational initiatives for all personnel 3. Best practices for cyber resilience should include but not limited to below key areas: a. Identification b. Protection c. Detection d. Response and Recovery e. Testing f. Learning and Reporting g. Situational Awareness
3.2.1	**Identification**	1. Organization shall establish and follow a cyber-threat intelligence process, analysis and information sharing process including but not limited: 2. The following Cyber threats shall be identified: a. That could affect the operational performance b. Cause significant impact to meet Organization 's objectives and obligations c. Cause threat to critical business, processes and reputation 3. Necessary steps shall be taken to identify assets that need to be protected on priority. a. Critical assets, business functions and processes shall be identified that shall be protected against compromise.

		b. Information assets (including sensitive personal information) and related system access shall be part of the identification process. c. Organization shall establish a process to gather and analyze cyber threat information in conjunction with internal and external business and system information sources d. Business process or Vendor risk shall be identified and assessed as a part of on-boarding and operations process. e. For detailed classification "Asset Management" section of "Information and Cyber Security policy" shall be referred.
3.2.2	**Protection**	1. Controls shall be in line with technical standards. 2. Resilience shall be provided by design. 3. 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. 4. Appropriate access controls on least privileges roles shall be part of application and access control design.
3.3.3	**Detection**	1. For critical systems cyber security monitoring is essential, as performing security events monitoring and or analytics shall assist in detection and mitigation of cyber incidents. 2. Please refer to 'Monitoring, Logging and Assessment Policy.'
3.3.4	**Response and Recovery**	1. Contingency planning, design, and business integration as well as data integrity are key enablers for fast recovery. 2. For effective contingency planning, periodic testing shall be conducted 3. Please refer "Incident And Problem Management Policy" and " Business Continuity Management and Disaster Recovery Policy"
3.3.5	**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".

<table>
<tr><td>3.3.6</td><td>Learning and Reporting</td><td>1. Organization shall continually re-evaluate the effectiveness of Cyber security management.
2. Organization 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.</td></tr>
<tr><td>3.3.7</td><td>Situational Awareness</td><td>1. Awareness contributes to the identification of cyber threats. Accordingly, the establishment of a threat intelligence process helps to mitigate cyber risk. In this regard, Organization shall participate in established information sharing initiatives as may require.
2. Cybersecurity awareness circulars and advisories shall be regularly sent to employees, third party vendor and consultants</td></tr>
<tr><td>3.4</td><td>Forensics</td><td>Organization may perform forensic investigations for incidents requiring investigation for legal or regulatory purposes and/or severe information security incidents. They may collect, process, store and analyze digital evidence in accordance with the regulations and laws</td></tr>
<tr><td>3.5</td><td>RACI Matrix</td><td><table><tr><td>Responsible</td><td>Accountable</td><td>Consulted</td><td>Informed</td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td></tr>
</table>

Policy No.:	2.21
Policy Name:	2.21 Email Security

1	**PURPOSE**	To define Organization's desired security requirements for protection of the electronic messaging used or controlled by Organization.
2	**SCOPE**	1. This policy shall apply to all communication channels and network connections through which Organization's information assets are transmitted. 2. Communications channels and network connections include but are not limited to E-mail, Internet, intranet and social media platforms 3. All Business Units or Departments using information technology must comply with these Information Security Policies
3	**POLICY**	1. Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities. 2. Organization may transfer information transfer through the use of a number of different types of communication facilities, including electronic mail, voice, facsimile and video. Software transfer may occur through a number of different mediums, including downloading from the Internet and acquisition from vendors selling off-the-shelf products. The business, legal and security implications associated with electronic data interchange, electronic commerce and electronic communications and the requirements for controls shall be considered. 3. Any breach of this policy shall be considered as an incident and shall be treated as per the incident management policy.
3.1	**Information security considerations for electronic messaging**	1. Organization shall to lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the Domain Keys Identified Mail (DKIM) standards. 2. DNS filtering services shall be used to help block access to known malicious domains.

<table>
<tr><td></td><td></td><td>3. Organization shall use sandboxing to analyse and block inbound email attachments with malicious behaviour.
4. Measures shall be implemented to control use of VBA/macros in MS office documents, control permissible attachment types in email systems</td></tr>
<tr><td>3.2</td><td>RACI Matrix</td><td><table><tr><td>Responsible</td><td>Accountable</td><td>Consulted</td><td>Informed</td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td></tr>
</table>

Policy No.:	2.22
Policy Name:	**2.22 Work from Remote Location**

1	**PURPOSE**	To define the roles, responsibilities and terms of use of Organization's information assets concerning Work from remote locations.
2	**SCOPE**	1. This policy shall apply to all employees, contractors and third-party who shall access Organization's information assets and facilities using remote connections. 2. All Business Units or Departments using information technology must comply with these Information Security Policies
3	**POLICY**	The objectives of this policy are to: 1. Prevent occurrence and recurrence of cyber incidents by implementing security proactive measures. 2. Create infrastructure for conformity assessment and certification of compliance to cyber security best practices, standards and guidelines 3. Create mechanisms for security threat early warning, vulnerability management and response to security threats 4. Create mechanism to prevent leakage of confidential information. Any breach of this policy shall be considered as an incident and shall be treated as per the incident management policy.
3.1	**Framework**	1. Board approved Cyber Security Policy (Policy) of the Insurer shall address risks associated with Work from Remote Location (WFRL) risks. The policy shall mandate the need to change passwords frequently. 2. Workflow approvals, deviations or exceptions shall be captured as per "*Change control policy- Section 2.9*" 3. Audit log monitoring and analysis shall be provisioned on organizational ICT infrastructure as a control for unauthorized access risks and cyber threats. 4. Evidences and artefacts shall be classified, securely demonstrated to concerned stakeholders and shall not be shared out of authorized domains.

		5. Project implementation documents, MIS reports shall be classified and shared on Need-to-know basis. 6. Insurance companies shall ensure that in the case of disruption IT support shall be accessed by investment application users through portal, help desk (phone) or email or visit to office.
3.2	**Network security**	1. Organization shall ensure a secure network with strong protocols and Wi-Fi passwords at remote location. 2. Authorized assets of the Organization provided to the users shall be hardened as per security policy for strong password authentication. 3. All servers, applications and networks shall be hardened and secured as per standardized security policy settings. 4. Device controls shall be implemented on user systems and Information and Communication Technology (ICT) infrastructure systems to block unauthorised internet domains, admin level access, unauthorized installation or changes to software, USB and other media, peripherals. 5. All user systems shall be enabled with Antivirus, Endpoint protection controls, data encryption and Data Loss Prevention mechanisms. 6. User systems and organization's ICT infrastructure shall be regularly updated with security patches and fixes. 7. Secure remote access mechanisms of Virtual Private Network (VPN), Internet Proxy or Virtual Device Interface (VDI) shall be provisioned for WFRL users accessing Organization data assets and applications 7. All patches, AV, End Point Protection, Data Encryption mechanisms shall be checked to ensure its appropriate functioning. 8. Applications shall be accessible ONLY to authorised users through a secured VPN access 9. Hardening procedures shall be put in place to check / scan systems brought back to office. 10. Controls shall be in place to identify unauthorized access, malicious code execution, suspicious activities or behaviour, credential theft, presence of advance persistent threats like remote access toolkits and such cyber risks to organizational infrastructure. 11. Email services shall be secured to prevent spam, spoofed mails and malware filtering and users shall be trained to handle spam, phishing scam and fraudulent emails.

		12. Suspicious or malicious domains on the internet shall be detected and blocked on network firewall, web proxy filtering, intrusion prevention systems 13. Security patch updates shall be reviewed and periodically applied on ICT infrastructure to prevent Distributed Denial of Services (DDoS) attacks. 14. DR Drill shall be performed to ensure adherence to Business Continuity metrics.
3.3	**Data management**	1. Data containerization, Multifactor authentication and remote data wipe shall be done to prevent data tampering and misuse of lost mobile/tablet devices during the period when WFRL has been permitted by the entity. 2. Users shall be mandated to back-up critical data periodically on secure location in organization systems. 3. Backups shall be reviewed periodically and procedures shall be aligned to minimize downtime impact.
3.4	**Human resource security**	1. Non-disclosure agreements / Undertaking on data security and confidentiality shall be signed at the time of employee/ consultant/ third-party vendor on boarding before permitting Operations to be commenced at WFRL. 2. Controls and procedures relating to secure access of Organization's data assets and applications from user-owned devices like mobile phones, tablets or other Bring Your Own Device (BYOD) shall be defined. 3. An audit of Privileged user identity access authentication shall be conducted for administrative purposes. 4. Activities like walkthrough and interviews shall be performed using approved remote access software over secure and hardened systems of auditee and auditor organizations.
3.5	**RACI Matrix**	Responsible | Accountable | Consulted | Informed [illegible]

Policy No.:	2.23
Policy Name:	2.23 Dealing room operations

1	**PURPOSE**	To define the roles, responsibilities and terms of use of Organization's information assets concerning operations in dealing room.
2	**SCOPE**	1. This policy shall apply to all employees, contractors and third-party who shall access Organization's information assets and facilities using remote connections. 2. All Business Units or Departments using information technology must comply with these Information Security Policies
3	**POLICY**	The objectives of this policy are to: 1. Create mechanism for secure recording of dealing information. 2. Create authorisation matrix in case of any deals to be carried out. 3. Create mechanism for record retention and consent to be obtained before entering into any contract. Any breach of this policy shall be considered as an incident and shall be treated as per the incident management policy.
3.1	**Data protection in IVR**	1. Dealers shall be provided with a dedicated and secured recording line during WFH for placing the calls to the brokers. 2. Insurance companies shall ensure that recorded lines are working and well maintained. 3. The Mid-office shall check voice recording as per a defined process in Standard Operating Procedure. 4. Voice logger shall be used for recording of calls made from office location. Back up/storage of such call recordings shall be enabled as a part of proof of transaction and the same shall be accessed anytime. 5. SOP shall define process to handle disruption in communication links between the dealers and brokers. 6. Communications between the dealers and brokers shall be logged/recorded and the same shall be independently reviewed by the Mid-office. 7. Dealers shall execute ALL transactions only through recorded telephone lines

		8. Secondary network connectivity and IT infrastructure shall be provisioned and tested for the critical applications and services.
3.2	**Authorization**	1. Dealing room operation procedure should be developed. 2. Policies / processes shall be defined to guide the officials of the Investments Function to process transactions with appropriate approvals in the event of disruption. 3. The SOP/Dealing room policy shall specify the dealers to places the orders only through empanelled brokers via authorized communication modes. 4. Appropriate prior approvals / authorisations shall be taken to process transactions with the brokers 5. Dealers shall ensure that emails are shared ONLY through authorized Organization email addresses registered with concerned counterparties. 6. Dealers shall ensure that IT support shall be accessed by Investment application users by way of portal, helpdesk or visit to office. 7. Supervisory monitoring process checklist which includes transaction price monitoring and trade monitoring etc shall be put in place. 8. Investment transactions shall be executed with requisite approvals defined as a part of Dealing Room Work flow / SOP. 9. Dealers shall completely disable the SMS / Chat facilities of all authorized Bloomberg terminals / Bloomberg. 10. Dealers shall execute all transactions via recorded telephone lines or authorized Bloomberg terminals / Bloomberg anywhere ID's / NDS terminals/TREPS terminals/Emails.
3.3	**Data security**	1. Voice recording analysis and rate scan shall be carried out on a regular basis to supervise trades and transaction price as defined in dealing room policy, 2. multi-factor authentication shall be enabled for all Bloomberg terminals. 3. Disaster Recovery (DR) Drills shall be performed to verify the availability of applications, processes and resources at remote backup site. The issues identified during such drills shall be addressed and documented.

		4. Contingency policy and plans, Backup/Alternative locations and resources shall be identified, revised and tested within Investment function periodically for an effective business continuity.					
3.4	**RACI Matrix**		Responsible	Accountable	Consulted	Informed	

Policy No.:	2.24
Policy Name:	**2.24 Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**

1	**PURPOSE**	To define the roles, responsibilities and terms of use of Organization's digital platforms
2	**SCOPE**	This policy shall apply to all employees, contractors and third-party who shall access Organization's information assets and facilities .
3	**POLICY**	The Objectives of this policy are to: 1. Create processes, structures and mechanisms to ensure data privacy. 2. Promote and launch a comprehensive awareness program on security of cyberspace. 3. Restrict any infringement of patent, trademark, copyright or other proprietary rights. 4. Due diligence to be considered while using social media
3.1	**Framework**	1. The rules and regulations, privacy policy or user agreement of the Organization shall inform the user of its computer resource not to host, display, upload, modify, publish, transmit, store, update or share any information that a. belongs to another person and to which the user does not have any right; b. is defamatory, obscene, pornographic, pedophilic, invasive of another privacy including bodily privacy, insulting or harassing on the basis of gender, libelous, racially or ethnically objectionable, relating or encouraging money laundering or gambling, or otherwise inconsistent with or contrary to the laws in force; c. is harmful to child; d. infringes any patent, trademark, copyright or other proprietary rights; e. violates any law for the time being in force; f. deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any information which is patently false or misleading in nature but may reasonably be perceived as a fact;

		g. impersonates another person; h. threatens the unity, integrity, defense, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognizable offence or prevents investigation of any offence or is insulting other nation; i. contains software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource; j. is patently false and untrue, and is written or published in any form, with the intent to mislead or harass a person, entity or agency for financial gain or to cause any injury to any person; 1. The Organization shall periodically inform its users, at least once every year, that in case of non-compliance with rules and regulations, privacy policy or user agreement for access or usage of the computer resource of such intermediary, it has the right to terminate the access or usage rights of the users to the computer resource immediately or remove non-compliant information or both, as the case may be. 2. The Organization on whose computer resource the information is stored, hosted or published, upon receiving actual knowledge in the form of an order by a court of competent jurisdiction or on being notified by the Appropriate Government or its agency under clause (b) of sub-section (3) of section 79 of the Act, shall not host, store or publish any unlawful information, which is prohibited under any law for the time being in force relation to the interest of the sovereignty and integrity of India; security of the State; friendly relations with foreign States; public order; decency or morality; in relation to contempt of court; defamation; incitement to an offence relating to the above, or any information which is prohibited under any law for the time being in force. 3. The Organization shall periodically, and at least once in a year, inform its users of its rules and regulations, privacy policy or user agreement or any change in the rules and regulations, privacy policy or user agreement, as the case may be. 4. The Organization which collects information from a user for registration on the computer resource, shall retained his information

		for a period of one hundred and eighty days after any cancellation or withdrawal of his registration, as the case may be. 5. The Organization shall take all reasonable measures to secure its computer resource and information contained therein following the reasonable security practices and procedures as prescribed in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011). 6. The Organization shall as soon as possible, but not later than seventy-two hours of the receipt of an order, provide information under its control or possession, or assistance to the Government agency which is lawfully authorized for investigative or protective or cybersecurity activities, for the purposes of verification of identity, or for the prevention, detection, investigation, or prosecution, of offences under any law for the time being in force, or for cyber security incidents. 7. The Organization shall report cyber security incidents and share related information with the Indian Computer Emergency Response Team in accordance with the policies and procedures as mentioned in the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013. 8. The Organization shall not knowingly deploy or install or modify technical configuration of computer resource or become party to any act that may change or has the potential to change the normal course of operation of the computer resource than what it is supposed to perform thereby circumventing any law for the time being in force. 9. The Organization shall publish on its website, mobile based application or both, as the case may be, the name of the Grievance Officer and his contact details as well as mechanism by which a user or a victim may make complaint against violation of the provisions of this rule or any other matters pertaining to the computer resources made available by it, and the Grievance Officer shall - a. acknowledge the complaint within twenty-four hours and dispose off such complaint within a period of fifteen days from the date of its receipt;

<table>
<tr><td></td><td></td><td>b. receive and acknowledge any order, notice or direction issued by the Appropriate Government, any competent authority or a court of competent jurisdiction.
10. The Organization shall within twenty-four hours from the receipt of a complaint made by an individual or any person on his behalf under this sub-rule, in relation to any content which is prima facie in the nature of any material which exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct, or is in the nature of impersonation in an electronic form, including artificially morphed images of such individual, take all reasonable and practicable measures to remove or disable access to such content which is hosted, stored, published or transmitted by it.</td></tr>
<tr><td>3.4</td><td>RACI Matrix</td><td><table><tr><td>Responsible</td><td>Accountable</td><td>Consulted</td><td>Informed</td></tr><tr><td></td><td></td><td></td><td></td></tr></table></td></tr>
</table>

Annexure A

Clause	Explanation
Information Technology (Amendment) Act,2008	IT (Amendment) Act 2008 has specified "reasonable security practices and procedures" to protect "sensitive personal data or information" (SPDI). It is mandatory to identify the SPDI processed and ensure all the process are compliant with IT (Amendment) Act 2008
Companies Act, 1956	This act requires various disclosures, filling and record keeping obligations to be fulfilled. Ensure compliance as regards availability, verifiability, authenticity, amenability to inspect, audit and review.
Insurance Act	To govern all form of insurance and to provide strict control over insurance business.
IRDAI Regulations	To aid, advise and assist insurers carrying on general insurance business in the matter of setting up equitable and clear standards of conduct and sound practice and in the matter of rendering efficient service to holder of general insurance guidelines.
Contract Act 1961	Determines the circumstances in which promises made by the parties to a contract shall be legally binding on them.
FERA/FEMA	Regulate the foreign payments, regulate the dealings in Foreign Exchange & securities and conservation of Foreign exchange for the nation
Stamp Duty Act	A tax that is levied on documents. Historically, this included the majority of legal documents such as cheques, receipts, military commissions, marriage licenses and land transactions.
Personnel Laws	Various personnel laws like the Payment of Wages Act, the ESI Act, Provident Funds Act etc. require various disclosures, filling and record keeping obligations to be fulfilled.
Digital Personal Data Protection Act	An Act to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.
Aadhaar Act	Aadhaar act aims to provide legal backing and governance to the Aadhaar unique identification number project.

Annexure B- RACI Matrix (Based on the Board Approved ICS Policy)

S.N	Policies	Asset Owner	HR	IT	Information Security	Admin	Finance	Business	Legal and Compliance	Risk Management Team	Vendors/ OEMs	Users	Change Requestor	Executive Management
1.	Data Classification													
2.	Asset Management													
3.	Access Control													
4.	Human Resource Security													
5.	Information System Acquisition and development													
6.	Information system and Maintenance													
7.	Change Control													
8.	Incident and problem management													
9.	Network Security													
10.	Cryptographic Controls													

S.N	Policies	Asset Owner	HR	IT	Information Security	Admin	Finance	Business	Legal and Compliance	Risk Management Team	Vendors/ OEMs	Users	Change Requestor	Executive Management
11.	Business Continuity Management													
12.	Third Party service provider													
13.	Physical and environmental security													
14.	Monitoring, logging and assessment													
15.	Mobile Device Security													
16.	BYOD													
17.	Legal and regulatory compliance													
18.	Situational Awareness													
19	Cloud Security													
20	Cyber Resilience													

Glossary

Term	Description
Insurance Company	Organization
ICSP	Information and Cyber Security Policy
IS	Information Security
ISRMC	Information Security Risk Management committee
ITSC	Information Technology Steering Committee
RMC	Risk Management Committee
IT Act	Information Technology (IT) Act
DPDP Act	Digital Personal Data Protection Act
RBI	Reserve Bank of India
IT	Information Technology
CRO	Chief Risk Officer
CISO	Chief Information Security Officer
HR	Human Resources
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 Agreements
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
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