# GUIDELINES ON INFORMATION AND CYBER SECURITY FOR INSURERS

**Table of Content**

# 1. Introduction

All insurers regardless of size, complexity, or lines of business, collect, store, and share with various third-parties (e.g., service providers, reinsurers etc.), substantial amounts of personal and confidential policyholder information, including in some instances sensitive health-related information.

Insurance repositories, call centers, Common Service Centers etc. also have access to policyholders' data.

While Information sharing is essential for conducting the business operations, it is essential to ensure that adequate systems and procedures are in place for ensuing that there is no leakage of information and information is shared only on need-to-know basis.

Further, due to rapid development Information Technology, there are many challenges in maintaining confidentiality of information. The technology even though has many advantages, brings in risks associated with it like any other technology. With the fast growth of web based applications, cyber threat landscape has been growing and there is concern across all sectors. Cyber risks have grown and cyber criminals have become increasingly sophisticated. For insurers, cyber security incidents can harm the ability to conduct business, compromise the protection of personal and proprietary data, and undermine confidence in the sector. It is observed that the level of awareness of cyber threats and cyber security within the insurance sector, as well as supervisory approaches to combat the risks, appear to vary across organizations.

Information obtained from regulated entities through cyber-crime may be used for financial gain through extortion, identity theft, misappropriation of intellectual property, or other criminal activities. Exposure of personal data can potentially result in severe harm for the affected policyholders, as well as reputational damage to insurance sector participants. Similarly, malicious cyber-attacks against an insurer's and Insurance Intermediaries' critical systems may impede its ability to conduct business.

Such security related issues have the potential to undermine public confidence and may lead to reputation risks to insurers. Hence, it is essential to ensure that a uniform framework for information and cyber security is implemented for insurers and an in-built governance mechanism is in place within the regulated entities in order to make sure that all such security related issues are addressed time to time.

# 2. Vision and Objective

(i) To ensure that a Board approved Information and Cyber Security policy is in place with all insurers.

(ii) To ensure that necessary implementation procedures are laid down by insurers for Information and Cyber Security related issues.

(iii) To ensure that insurers are adequately prepared to mitigate Information and cyber security related risks.

(iv) To ensure that an in-built governance mechanism is in place for effective implementation of Information and cyber security frame work.

# 3. Applicability

This guidelines document is applicable to all insurers regulated by Insurance Regulatory and Development Authority of India (IRDAI).

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

The “Control Check List” is provided in **Annexure A**.

# 4. Terms &Definitions

| | |
|---|---|
| **Admin** | Administration |
| **BCM/BCP** –. | Business Continuity Management/Plan |
| **BYOD** | Bring Your Own Device |
| **CA** | Certification Authority |
| **CCA** | Controller of Certifying Authority |
| **CERT In** | Computer Emergency Response Team - India |
| **CCMP** | Comprehensive Cyber crisis Management Plan |
| **CIO** | Chief Information Officer |
| **CIA** | Confidentiality, Integrity and Availability |
| **CISA** | Certified Information Systems Auditor |
| **CISO** | Chief Information Security Officer |
| **CRO** | Chief Risk Officer |
| **DDoS** | Distributed Denial of Service |
| **DISA** | Diploma in Information Systems Audit |
| **DLP** | Data Loss Prevention |
| **DR** | Disaster Recovery |
| **HR** | Human Resource |
| **IDS** | Intruder Detection System |
| **IMEI** | International Mobile Equipment Identity |
| **IPS** | Intruder Prevention System |
| **IRDAI** | Insurance Regulatory and Development Authority of India. |
| **IRM** | Information Risk Management |
| **ISC** | Information Security Committee. |
| **MAC** | Media access control |
| **NCIIPC** | National Critical Information Infrastructure Protection Centre |
| **NDA** | Non -Disclosure Agreement |
| **OEM** | Original Equipment Manufacturer |
| **Organization** | Insurance company registered with IRDAI |
| **PII** | Personally identifiable information |
| **SCD** | Secure Configuration Document |
| **SLA** | Service Level Agreement |
| **SOC** | Security Operations Centre |
| **SOP** | Standard Operating Procedure |
| **VLAN** | Virtual Local Area Network |
| **VM** | Virtual Machine |
| **VPN** | Virtual Private Network |

# 5. Enterprise Security

## 5.1 Governance, Policy & Standards, Strategy

The organization shall adopt, direct, monitor and communicate an information and Cyber security policy/policies (herein after referred to as 'IS Policy'), approved by the Board in order to ensure that the organization's overall objective to information security is achieved.

## 5.2 Establishment of governance framework

The Framework for information security governance shall be established by the organization.

## 5.3 Chief Information Security Officer (CISO)

Every Organization shall appoint/ designate a suitably qualified and experienced Senior Level Officer exclusively as Chief Information Security Officer (CISO) who will be responsible for articulating and enforcing the policies to protect their information assets.

## 5.4 Roles and responsibilities of CISO

a) Responsible for articulating Information and Cyber Security policy for the Organisation
b) Be responsible for providing advice and support to management and information users in the implementation of Information and Cyber Security Policy.
c) Build and lead the information security team with appropriate competencies and attitude to deliver the information security program.
d) Promote user awareness initiatives within the organization.
e) Propose Information and Cyber Security Policy to the ISC, incorporate feedback on the implications of the policy from the ISC and other business areas into the policy-making process.
f) Be responsible for providing advice and support to management and information users in the implementation of Information and Cyber Security Policy.
g) Build and lead the information security team with appropriate competencies and attitude to deliver the information security program.
h) Promote user awareness initiatives within the organization.

The CISO shall to report to the Head of Risk Management and will have a working relationship with the CIO to develop the required rapport to understand the IT infrastructure and operations, to build effective security in IT across the organization, in tune with business requirements and objectives. The organization shall ensure segregation of duties for Information Security & IT operations.

### 5.5 Information Security Committee (ISC)

The organization shall form an Information Security Committee (ISC) headed by a senior level executive with a reporting line to the Board to take overall responsibility for the information security governance framework.

Members of ISC shall include functional heads from Operations, Information Technology, Legal, Compliance, Finance, HR, Risk etc.

The Information Security Committee (ISC) shall:

a) Review and recommend to the Board necessary changes to the high level IS Policy. The Committee shall approve standards and procedures in line with the Board-approved IS policy. Individual business functions should create and get their SOP's approved (in line with above standards & procedures) by the respective functional heads.

b) Review and approve exceptions to the Information Security Policy, any significant risk to be reported to the Board. However Operational level exceptions can be approved by Respective Business owner in consultation with CISO.

c) Recommend changes to the constitution and functioning of the committee.

d) Review, discuss and direct information security risk mitigation (which includes reporting security incidents) and ensure that risks are accurately reported and appropriately dealt with.

e) Ensure compliance to regulatory and statutory requirements related Information Security.

f) Be responsible to ensure management of cyber security initiatives and incident management.

g) The ISC shall ensure that the information security governance framework is supported by an information security assurance programme (Implementation Plan).

h) ISC should report to Risk Management Committee of the Board a minimum of two times in a year.

i) CISO shall be convener of the Information Security Committee.

### 5.6 Role of the Board

The Board shall demonstrate their commitment by approving:

- The overall framework to information and cyber security policy and strategy
- The information and cyber security assurance programme.

### 5.7 Heads of functional Departments

Each functional Head shall provide leadership and sponsorship to the agreed security program by driving the same to the teams under their management and mandate compliance. Individual functional head will be responsible for implementation of information and cyber security management related policies.

### 5.8 Information Security Team

Organizations shall form a separate information security Team to focus exclusively on information security management. There should be segregation of the duties of officials dealing exclusively with information systems security and the Information Technology Division which actually implements Information Security controls at operational level. The organization of the information security function should be commensurate with the nature and size of activities of the organization. The information security team should be adequately resourced in terms of the number of staff, level of skills and tools or techniques like risk

assessment, security architecture, vulnerability assessment, forensic assessment, etc. While the information security team, its functions and information security governance related structures should not be outsourced, specific operational components relating to information security may be outsourced, if required resources are not available within an Organization. However, the ultimate control and responsibility rests with the organization.

Information Security team shall: -

a) Develop and maintain IS policy, standards, procedures and guidelines to support the organizations' information security program.
b) Translate the information security program into specific actions which shall include awareness, security infrastructure, security incident response and risk management.
c) Work closely with IT and other functional teams and monitor implementation of information security projects and controls for new or identified deficiencies.
d) Identify current and potential legal and regulatory issues affecting information security and assess their impact in conjunction with legal and compliance team.
e) Act as consultants and advisors to different stakeholders for information security matters.
f) Perform information security risk assessments on an ongoing basis and report any significant risks to ISC.
g) Monitor information security incident management i.e. identification, response, remediation and reporting.

**5.9 Implementation**

**5.9.1 Technology/Operations/Admin/HR/ Functional teams shall –**

a) Have primary responsibility for ensuring that appropriate and adequate security mechanisms are provided in the systems and network infrastructure shared across systems and business units.
b) Be responsible for agreeing to security classification of all infrastructure components in agreement with the business owners.
c) Have primary ownership to comply with specific security policies, which will be applicable for systems development and acquisition.
d) Be responsible for maintenance of the various security tools and solutions.
e) Be responsible for monitoring of secure status on each system and network within its control. Report on weaknesses or breaches of security to be made to the relevant

Business owners or Infrastructure owners and to the CISO, who shall in turn co-ordinate, the incident response.

f) Technology/Operations/Admin/HR/ functional teams shall designate a suitable and qualified team member who will be responsible for reporting the incidents & effectiveness of security control to CISO /Information Security Team/ CIO.

g) Legal Team — Legal Team is responsible for Engagement with Cyber security police officials, lawyers and Government agencies as required. Necessary details with regards to the incident are provided by information security team.

h) Users and Information Owners — System users and data owners are responsible for the application of the policies relating to the systems, data, and other information resources under their care or control. They are also responsible for reporting any suspected cyber security incident to Information Security Team/IT Head.

**5.9.2 Responsibilities of Business Owners:**

Business owners shall

a) Hold the primary responsibility for defining the value and classification of assets within their control by participating in the risk management process and undertaking business impact assessment. b) Be responsible for authorizing access and segregation of duties for individual users and groups including Third parties to the information contained within the applications.

b) Ensure that appropriate access of administration roles or teams exist for their applications to administer access in accordance with the IS Policy.

c) Ensure implementation and compliance to Information Security Policies as applicable for their business units.

d) Be primarily responsible for risk, data security and access of Third party partners and vendors to whom line of business has been outsourced

e) Review the self-assessment of Third parties at defined frequency to whom line of business has been outsourced.

f) Be responsible for conducting security assessments and audits of Third party processes / sites)

g) Define Information Security requirements for third parties in concurrence with the Information Security team of the organization

**5.10 Conformance**

**Users of following category shall be responsible for complying with the IS Policy**

a) Senior management's primary responsibility shall be to develop a clear business aligned program for information security, assign roles and responsibilities, support the IS Policy and provide sponsorship and budget to ensure it is successfully practiced.

b) Information user's primary responsibility shall be to practice information security by working within the IS Policy and report promptly any unusual suspected or detected attempts to breach security.

**5.11 Enforcement**

**5.11.1 Internal Audit Shall**

a) Internal Audit plan of the organization shall have a separate IS audit plan covering IT/Technology infrastructure and applications. The audit plan and the reports shall be presented to the Audit Committee of the Board
b) Conduct audit for third party /vendors handling critical data on planned and ad hoc basis to measure the effectiveness of the third party security controls implemented.
c) All instances of non-compliance related to Information security shall be communicated and discussed with relevant line management and CISO.

**5.11.2 CISO shall**

a) Provide the management and Users assistance in correcting deficiencies.
b) Bring significant issues on non-compliance to the attention of the ISC for review and remediation.
c) Initiate / undertake an ongoing or ad hoc third party review/assessment of a specific function or a product to measure the effectiveness of the controls implemented and highlight any vulnerability that needs to be fixed.

**5.11.3 Functional technology teams shall –**

a) Be responsible for undertaking regular monitoring of secure status on each system and network within its control.
b) Report on weaknesses or breaches of security to the relevant Business Owners or Infrastructure Owners and to the CISO, who shall be responsible to manage the incident response.
c) Responsible for driving end point system and server security.

**5.12 Awareness**

All stakeholders (employees, contract staff etc.) are made aware of organizational information security policies, procedures and guidelines, threat exposures etc. They should be aware of their roles, responsibilities and abide by them to reduce the risk of human error.

**5.12.1 Information Security Awareness: -**

a) Sufficient means including technology shall be employed to create an understanding, familiarity and recognition of the business & Information security objectives and direction, as captured in the IS Policy, through communication to appropriate stakeholders and users throughout the organization.
b) Educating vendors and employees on information security do's and don'ts when using technology facilities and delivery channels.
c) Provide general and specific information about cyber security risk trends, types or controls and make them aware of their responsibilities in relation to fraud prevention.

**5.13 Training**

The organization shall ensure that all personnel who are assigned the responsibilities are competent to perform the required tasks and provided with regular training.

**5.13.1 Information Security Training Goals**

All employees and, where applicable, contract staff, 3rd party service providers and vendors shall receive appropriate information security awareness training or periodic updates as relevant to their function to ensure secure business operations

### 5.14 Identity and Access Management

Identity management and access control arrangements shall be established to provide effective and consistent user administration by establishing identity accountability and authentication to allow business applications/systems/ networks/computing devices access to only authorized 'users'.

### 5.14.1 Establish security and access control policies & procedure

**a) Access control mechanisms should:**

I. Limit access in line with access policies set by owners of business applications and systems.
II. Restrict the business application/system/ network/computing device capabilities that can be accessed (e.g. by providing menus /groups that enable access only to the particular capabilities needed to fulfill a defined role)
III. Supplement passwords (e.g. by using strong authentication such as smartcards, biometrics or tokens), if and when necessary.
IV. Minimize the need for special access privileges (e.g. User IDs that have additional capabilities, such as 'Administrator', or special capabilities, such as User IDs that can be used to authorize payments)
V. Require approval/s business application/system/ network/ computing device from appropriate authority to provide access privileges for both business users and computer staff.
VI. Have a process for terminating the access of normal users as well as privileged users.
VII. Be reviewed on Periodic basis
VIII. Details of Business owner, approvers and their delegated authority shall be maintained and be re-certified and updated periodically. The authorization process shall include process for granting emergency access

**b) Privileged access -**

Additional controls should be applied to special access privileges, including high level privileges (e.g. 'root' in Unix or ‘Administrator' in Windows systems/powerful utilities and privileges that can be used to authorize payments or perform financial transactions)

**(c) Authentication & password synchronization**

All ‘Users’ shall be authenticated at a minimum by using User IDs and passwords, before they can gain access to target systems to prevent Unauthorized access to the Organization’s information assets.

**(d) Provisioning and de-provisioning**

Repository for all users including third parties should be maintained.

**5.14.2 Effective user group management –**

**a) Modification/ Deletions-group: -**

i) Access shall be timely modified as required when 'Users' moves internally

ii) Access shall be timely revoked when 'Users' exits

**b) Re-certifications -**

i) All user-IDs and their access right shall be reviewed by the respective functional business owner on a regular basis to avoid existence of stray/orphan user accounts and ensuring that access rights are based on the need to know basis principle.

ii) The review shall include verification that the user's access rights and privileges are still in line with job requirements.

**c) Generic IDs-**

**i)** Generic User-Ids/Service IDs shall be avoided and where no alternative exists, it shall be controlled, authorized by Business/Asset Owner, to avoid misuse to compromise user accountability.

**ii)** Privilege generic user-IDs shall allow the user to only perform the intended activities for which the user-IDs was created. Such IDs shall be authorized by business/Asset owners

**d) Remote Access-**

i) Remote access to the Organization's infrastructure shall be highly restricted and controlled to prevent unauthorized access to the Organization's infrastructure from untrusted networks

ii) 'Users' seeking to gain privileged access to the Organization's IT facilities via public or other external networks shall do so via two factor authentications.

**5.15 Change Management**

Changes to business applications, computer Systems and networks shall follow a change management process covering associated Risks, Change authorization, Business Continuity and impact.

a. A change management process shall be established, which covers all types of change (e.g. upgrades and modifications to application and software, modifications to business

information, emergency 'fixes' and changes to computer systems and networks).

b. The change management process shall be documented, and include approving and testing changes to ensure that:

i) They are made correctly and securely

ii) They do not compromise security controls

iii) No unauthorized changes have been made and only approved changes are released in production

iv) Version control is maintained so that it can be rolled back if required.

v) Authorized person should be allowed to make changes on the production system.

**5.16 Change Implementation**

a) There shall be implementation plan for executing a change that includes but not limited to:

i) Implementation steps

ii) Downtime requirements/Project plan.

iii) Test plan

iv) Roll back Plan

b) All changes shall be monitored and reviewed for successful implementation and documented, they shall:

i) Be performed by skilled and competent individuals who are capable of making changes correctly and securely. Developer and Release Manager / Deployment team access should be segregated.

ii) Be signed off by appropriate business owners.

iii) Have a record of version control and capture what was changed when and by whom.

iv) Have communication of details to relevant individuals and checks be performed to confirm that only intended changes have been made

v) Ensure that documents associated with computer systems and networks are updated.

c) Adequate control shall be implanted to ensure data integrity and confidentiality during/after data migration and its completeness shall be verified.

d) Digital records created are to be adequately preserved over time and remain accessible and functional, even over successive changes in technology.

**5.17 Vendor/Third party Risk Management**

Information security requirements shall be considered at all stages throughout third party/vendors having access/handling the organizational system/data.

### 5.17.1 External party management

There shall be a process for managing the security of relationships with external parties. The vendor risk management process shall involve the information security function, and include

i. Agreeing security arrangements (e.g. based on business security requirements and the relationship with third compliance needs) for each external party with security team.
ii. All arrangements with external party/vendors shall have a well-defined service level agreement (SLA) that shall specify information security requirements and controls, service levels and liability of suppliers in case of SLA violations, non-mitigation of IS vulnerabilities, IS incidents etc. External party shall demonstrate compliance with all SLA requirements.
iii. Validating security arrangements for each vendor.
iv. Handling termination of a relationship with a vendor.
v. Sub-contracting arrangements should cover due diligence aspects
vi. Right to audit /inspection.

However, the ultimate responsibility lies with the organization.

### 5.17.2 Addressing risks related to external Parties

The risks to the Organization's information and related information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented in following scenarios.

#### 5.17.2.1 Prior to Engagement

i) External parties shall be subject to a relationship assessment (sometimes referred to as due diligence review) shall cover:

a) Dealing with the said party (e.g. details of provider history, previous and current business arrangement and dispute information)
b) Contract requirements shall include non-disclosure agreements, sub-contracting, roles and responsibilities, and termination clauses and right to inspect/audit by Organization, Law enforcement agencies and regulating agencies including IRDAI
c) Third party demonstrable level of maturity in relation to information security and their degree of commitment to information security. This is via a self-assessment checklist covering their maturity in the area

ii) Risk assessment shall be conducted for determining the risks involved in granting access

to third parties to Organization's information/information systems.

iii) The list of security controls shall be determined to be implemented based on the type of engagement and nature of information sharing requirement.

iv) Data should be shared ONLY on "Need to know" basis

#### 5.17.2.2 During Engagement

Security Performance and Access Management:

i. Confidentiality and non-disclosure agreements with third parties shall be reviewed periodically and whenever the service terms and conditions are changed.

ii. Access management for third parties including granting access, review of user access rights shall be periodically assessed and changed as applicable.

iii. In case of third party including Call Centre operations, the Operating system has to be hardened to prevent data leakages.

iv. External Party Internal Controls Review:

a) External parties requiring review of internal control shall be identified on a periodic basis

b) Review findings shall be communicated to external party and corrective action shall be monitored.

#### 5.17.2.3 Termination or renewal of Engagement

i) A consistent method for securely handling the termination of relationships with Parties shall be established which shall include:

a) Designating individuals responsible for managing the termination

b) Revocation of physical and logical access rights to the organization's information

c) Return, transfer or secure destruction of assets (e.g.' back-up media storage' documentation, hardware and data.)

d) Coverage of license agreements and intellectual property rights

ii) In case of renewal, revisit the security considerations in line with the Prior to engagement scenario.

**5.18 Business Continuity Plan**

Alternative (contingency) arrangements shall be established to ensure that the organization's business processes can continue in the event that the external party is not available (e.g. due to contract termination or a disaster or a dispute with the external supplier or the entry ceases its operations). This arrangement shall be based on the results of a risk assessment:

The provision of alternative, secure facilities for business processes to continue

i. Organization to evaluate Escrow for information systems source code for and end of support / proprietary technologies (e.g.' application source code and cryptographic keys) using a trusted external party, such as a legal representative, lawyer or equivalent.
ii. Recovery arrangement to ensure continued availability of information stored at an outsource Provider.
iii. Alignment with the organization's business continuity program.

# 6. Information Asset Management

Objective: To identify organizational assets, define appropriate protection and responsibilities. Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained. The asset inventory should be accurate, up to date.

For each of the identified assets, ownership of the asset should be assigned and the classification should be identified.

The asset owner should:

a. Ensure that assets are inventoried;
b. Ensure that assets are appropriately classified and protected;
c. Define and periodically review access restrictions and classifications to important assets, taking into account applicable access control policies;
d. Ensure proper handling when the asset is deleted or destroyed.

All employees and external party users should return all of the organizational assets in their possession upon termination of their employment, contract or agreement.

The termination process should be formalized to include the return of all previously issued physical and electronic assets owned by or entrusted to the organization.

In cases where an employee or external party user purchases the organization's equipment or uses their own personal equipment, procedures should be followed to ensure that all relevant information is transferred to the organization and securely erased from the equipment.

An appropriate set of procedures for information labeling should be developed and implemented in accordance with the information classification scheme adopted by the organization.

Media should be disposed of securely when no longer required, using formal procedures.

# 7. Physical and environmental security

Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

Security perimeters should be defined and used to protect areas that contain either sensitive or critical information, and information processing facilities.

Physical barriers should, where applicable, be built to prevent unauthorized physical access.

Surveillance systems shall be in place and regularly monitored to cover all major areas

Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

Access rights to secure areas should be regularly reviewed and updated, and revoked when necessary.

Appropriate controls shall be implemented to manage calamities like fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster.

Mock drills shall be conducted periodically to test the effectiveness of the controls.

IT equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.

Users should ensure that unattended equipment has appropriate protection.

Secure computers or mobile devices from unauthorized use by a key lock or an equivalent control, e.g. password access, when not in use.

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.

## 8. Human resource security

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

Information security roles and responsibilities should be communicated to job candidates during the pre-employment process.

A code of conduct may be used to state the employee's or contractor's information security responsibilities regarding confidentiality, data protection, ethics, appropriate use of the organization's equipment and facilities, as well as reputable practices expected by the organization.

Awareness, education and training activities should be suitable and relevant to the individual's roles, responsibilities and skills.

There should be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

# 9. System acquisition, development and maintenance

Objective: To ensure that information security is an integral part of information systems across the system development lifecycle.

Identification and management of information security requirements and associated processes should be integrated in early stages of information systems projects. Early consideration of information security requirements, e.g. at the design stage can lead to more effective and cost efficient solutions.

Criteria for accepting products (software & solutions) should be defined e.g. in terms of their functionality, which will give assurance that the identified security requirements are met. Products should be evaluated against these criteria before acquisition.

# 10. Information Security Risk Management

Objective: To enable individuals who are responsible for target environments to identify key information risks and determine the controls required to keep those risks within acceptable limits.

Policy Procedure and Guidelines: The Organization should have a risk management program to undertake information security risk assessment for target environments (e.g. critical business environments, business processes, business applications, computer systems and networks) on a periodic basis

## 10.1 Managing Information Security Risk Assessment

**10.1.1** There shall be formal, documented standard/procedures for performing information risk assessments, which apply across the organization. Standards procedures to cover

a. Need for information security risk assessment
b. Types of target environment that would be assessed for information risks, e.g. IT Applications, hardware and software, vendors, etc.
c. Circumstances in which information assessments will be performed
d. Individuals that need to be involved and their specific responsibilities – business owners, experts in risk assessment, IT, etc.
e. Method of managing and mitigating to the results of information risk assessments

**10.1.2** Results from information security risk assessments conducted across the organization to be:

a. Reported to business owners and senior management or equivalent
b. Used to help in information security program
c. Integrated with wider risk management activities
d. Establish Information Security Risk Management
e. Define the scope of Information Risk Management(IRM)
f. Define a systematic approach to risk assessment
g. Identify the risk to assets within the scope of IRM
h. Assess the risks, Identify and evaluate options for the treatment/remediation o frisks
i. Select control objectives and controls for the treatment of risk Implement and Operate Information Risk Management

j. Formulate and implement a risk treatment plan
k. Implement the controls selected to meet the control objectives.
l. Manage the IRM related operations and resources
m. Implement procedures and other controls to detect and respond to the security incidents
n. Monitor and Review Information Risk Management

**10.1.3 Execute monitoring procedures and other controls to:**

a. Detect errors in the results of processing promptly
b. Identify failed and successful security breaches and incidents promptly
c. Enable management to determine whether the security activities delegated to people or implemented by information technology are performing as expected
d. Determine the actions taken to resolve a breach of security, reflecting business priorities
e. Undertake regular reviews of the effectiveness of the IRM work plan
f. Review the level of residual risk and acceptable risk
g. Maintain and Improve Information Risk Management
h. Implement the identified improvements in the IRM work plan
i. Take appropriate corrective and preventive actions
j. Communicate the results and actions to concerned teams and consult with CISO on improvement plans
k. Ensure that the improvements achieve their intended objective

**10.2 Information Security Policy - Acceptable Use**

Information, regardless of its form, is a valuable asset for the organization. The objective of the information security policy is to ensure confidentiality, integrity and availability of information. To instill security culture among all employees that supports the organization's information security policy and information security strategy. The information security policy shall cover elements on the acceptable use for the end users which will help build a secure environment across the organization.

The acceptable use policy shall cover:

- Information classification and labeling
- Password management
- Endpoints (desktop/laptop and mobile devices)
    - Standard configuration disabling vulnerable services and resources Virus/Malware protection

- Controls to prevent installation unauthorized/non- standard software
- Logical access
- Clear desk
- Internet access policy
- Email policy
- Usage of external/portable storage devices
- Instant messaging and social media
- Remote access
- Wireless access

**10.3 Business Continuity & Disaster Recovery Framework**

**10.3.1 Business continuity policy& Management**

a. The Organization shall have a Business continuity policy, with clearly identified responsibilities
b. BCP should be a key aspect of the Organization's Risk Management
c. The Policy shall be communicated to all the persons involved with or responsible for business continuity at various levels in the Organization
d. The Policy shall be reviewed at periodically or in case of any significant changes
e. Necessary resources like work area and manpower, etc. to be provided for effective BC implementation and operation

**10.3.2 Business continuity awareness**

a. The BC policy to be communicated and available to the employees
b. Staff training programs for the concerned employees

**10.3.3 The BCP should contain the following:**

a. Business impact analysis
b. Business continuity strategy/plan
c. Emergency response plan
d. BCP testing reports

**10.3.4** Business impact analysis to be conducted to identify the critical business processes, resources needed to support them and the impact measurement in time in case of unavailability

**10.3.5** There shall be a defined method for determining the impact of any disruption to key business processes

**10.3.6** The Organization shall identify suitable Business Continuity arrangements to recover identified critical activities within acceptable time.

**10.3.7** Supporting systems or processes (Non-Critical) required at DR should be identified and recovery planned with acceptable tolerance levels.

**10.3.8** The Organization shall develop Emergency response structure that will manage incident and ensure continuity of its critical activities

**10.3.9** The Organization shall validate the on-going effectiveness of its Business Continuity planning via periodic testing and Prepare the report of the exercise, outcome and learning including required actions

**10.3.10** The Management **shall review the Organization's business continuity preparedness at planned** intervals or when significant changes occur

# 11. Data Security

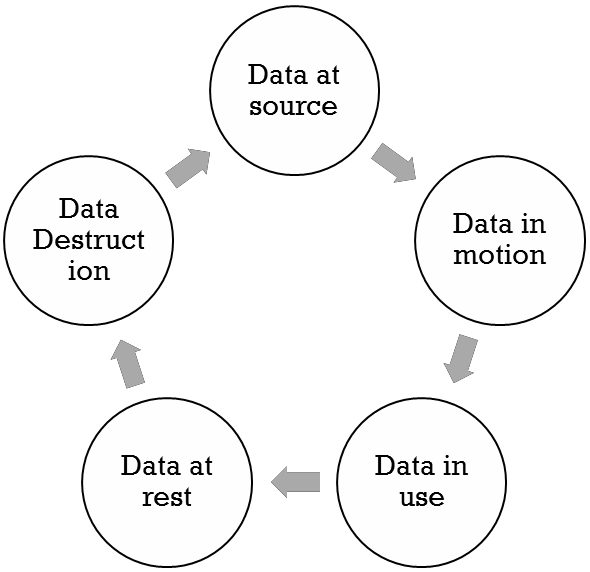
**Objective:** Organizations shall recognize that the efficient management of its data security is necessary to support its core functions, to comply with its statutory and regulatory obligations and to contribute to the effective overall management.

**Scope:** Organizations need to define and implement procedures to ensure the Confidentiality, Integrity, Availability and Consistency of all data stored in different forms. These guidelines are applicable to all information/records/data created, received or maintained by all permanent and temporary employees and consultants (collectively "the employees"), third party vendors of the organization and business distributors who have access to the organization's data, wherever this data records are and whatever form they are in, in the course of carrying out their designated duties and functions

### 11.1 Scheme of the data security policy

An overview of recent megatrends like emerging consumerization, the rise of cloud computing, increased importance of business continuity, enhanced persistence of cybercrime and increased exposure to internal threats shows that data protection will continue to be a significant challenge for organizations resulting in increasing data risk.

Information as data has a natural lifecycle, from creation and origination through storage,




processing, use and transmission to its eventual destruction or decay. The value of, and risks to, data assets may vary during their lifetime, but data security remains important to some extent at all stages.

Hence at every stages of data life cycle, organizations shall ensure due care of security to the Confidentiality, integrity and availability. Following data security controls to be considered as

mentioned below:

- Consistency & accuracy of data entered into the system should be verified through a maker checker process wherever applicable. There should be a process to ensure that such maker/ checker functions for conflicting roles follow segregation of duties and the same user cannot perform both the functions
- Audit trail of critical data access shall be maintained. Audit trails should be secured to ensure the integrity of the information captured, including the preservation of evidence. Retention of audit trails should be in line with business, regulatory and legal requirements.
- Access should be provided on “Need to Know” or “Least Privileges” based to ensure that necessary personnel (Employee) have access to essential system & this access should be reviewed periodically.
- For data generated /created on paper, user shall ensure that it follows data classification policy, stores it in a safe place in the office and maintain the CIA of data.
- Organizations should have a process to verify job application information on all new employees. Organizations should verify that contractors are also subject to similar screening procedures
- When deciding upon protection of specific organizational data records, their corresponding classification based on the organizations classification scheme, should be considered. Once the data is classified, it shall be the responsibility of users to ensure that adequate controls followed as per policy and an inventory of critical data storage locations shall be identified & documented
- In order to secure business sensitive/ critical data, a mechanism to identify critical data based on its impact to the business shall be defined.
- Regular awareness program to the users about handling of the critical data, classification levels of data shall be imparted on regular basis.
- Confidentiality undertaking shall be obtained from the users
- The critical data on the laptops and other mobile devices shall be protected to avoid disclosure of data in case of loss of the laptop or other devices.
- There should be secure storage of media. Controls could include physical and environmental controls such as fire and flood protection, limiting access by means like physical locks, keypad, passwords, biometrics, etc., labeling, and logged access.
- Cryptographic/password management techniques need to be used to control access to critical and sensitive data/information in transit and storage.

- Sensitive data if required to be sent to outsource services provider, third party for business purpose, shall be approved by the information/ business owner and controls are designed to ensure that data shall not be misused by the third party. (NDA, right protected email, etc.)
- Adequate controls to maintain data integrity and confidentiality while data is being archived shall be maintained. When archived in storage, the data should have proper access controls.

Disposal mechanisms should ensure the effective destruction of data. Such mechanisms include digital file shredding, degaussing (i.e. the process of demagnetizing magnetic media to erase recorded data) and physical destruction of storage media (e.g. pulverization, incineration or shredding). Reformatting may also be used as a method of destruction if it can be guaranteed that the process cannot be reversed. To ensure the complete destruction of a digital record, all extant copies should be located and destroyed. This includes removing and destroying copies contained in system backups and offsite storage.

# 12. Application Security

**Objective:** To ensure that information security is an integral part of information systems across the entire lifecycle and also includes the requirements for information systems which provide services over public networks.

The following are the important Application control and risk mitigation measures which should be considered for implementation by the Organization:

**12.1 Each application to have an owner.**

Some of the roles of application/business owners shall include:

a) Prioritizing any changes to be made to the application and authorizing the changes
b) Deciding on data classification/de-classification and archival/purging procedures for the data pertaining to an application as per relevant policies/regulatory/statutory requirements in agreement with business owners
c) Ensuring that adequate controls are built into the application through active involvement in the application design, development, testing and change process
d) Ensuring that the Change Management process is followed for any changes in the application
e) Ensuring that the application meets the business/functional needs of the users
f) Ensuring that the security of the application has been reviewed
g) Taking decisions on any new applications to be acquired / developed or any old applications to be discarded
h) Informing the information security team regarding purchase of an application and assessing the application based on the security policy requirements
i) Ensuring that the new applications being purchased/developed follow the Information Security policy
j) Ensuring that logs or audit trails, as required, are enabled and monitored for the applications. Logs should at least meet who-when-what-where criteria based on criticality.
k) Maintain last login details for all internet portal applications
l) Ensure review of access and roles are conducted periodically

**12.2 Information security requirements analysis and specification**

a) The information security related requirements are included in the requirements for the development of the new information systems or enhancements in the existing information systems

b) Besides business functionalities, security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, security event tracking and exception handling are required to be clearly specified at the initial stages of system development/acquisition

c) There should be a proper linkage between a change request and the corresponding action taken

d) Any changes to an application system/data need to be justified by genuine business need and approvals supported by documentation and subjected to a robust change management process.

**12.3 Technical review of applications after operating platform changes**

When operating platforms are changed, business critical applications to be reviewed and tested to ensure that there is no adverse impact on organizational operations or security

**12.4 Secure system engineering principles**

a. Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts

b. There should be documented standards/procedures for administering the application and updated periodically

c. Potential security weaknesses / breaches should be identified. There should be measures to reduce the risk of theft, fraud, error and unauthorized changes to information through measures like supervision of activities and segregation of duties

d. Applications must not allow unauthorized entries to be updated in the database. Similarly, applications must not allow any modifications to be made after an entry is authorized. Any subsequent changes must be made only by reversing the original authorized entry and passing a fresh entry.

e. Robust input validation controls, processing and output controls needs to be built in to the application. Validations should be included on all critical pages so that attacks are minimized and no manipulation can be allowed to change data at source

f. Critical Applications to provide for, logging unsuccessful logon attempts, access to sensitive options in the application, e.g., master record changes, granting of access rights, use of system utilities, changes in system configuration, etc.

g. The audit trails need to be stored as per a defined period as per any internal/regulatory/statutory requirements and it should be ensured that they are not tampered with

**12.5 Secure development environment**

a. Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development life-cycle
b. The development, test and production environments need to be properly segregated, any exceptions to be signed off by the ISC.
c. **Access should be based on the principle of least privilege and "need to know" commensurate with the job responsibilities**. Adequate segregation of duties needs to be enforced

**12.6 Outsourced development**

The IT/Business team should review the activity of outsourced system development. Organization may obtain **application integrity statements in writing from the application system vendors** providing for reasonable level of assurance about the application being free of malware at the time of sale, free of any obvious bugs, and free of any covert channels in the code (of the version of the application being delivered as well as any subsequent versions/modifications done).

**12.7 System functionality and security testing**

Testing of security functionality to be carried out

a. All application systems to be tested during the implementation in a robust manner regarding functionality controls to ensure that they satisfy business policies/rules of the organization and regulatory and legal prescriptions/requirements
b. Robust system based controls need to be built into the system and thereby reducing the reliance on any manual controls
c. All applications to be tested for security controls to check for known vulnerabilities initially and during major changes.
d. Before the system is live, there should be clarity on the audit trails and the specific fields that are required to be captured as part of audit trails and an audit trail or log monitoring process including personnel responsible for the same.

**12.8 Others**

a. Direct back-end updates to database should not be allowed except during exigencies, with a clear business need and after due authorization as per the relevant policy.
b. Applications should be configured to logout the users after a specific period of inactivity
c. There should be suitable interface controls in place to prevent any unauthorized modification
d. Establish a suitable backup policy for the application

# 13. Cyber Security

**Objective:** To raise awareness and provide guidelines to organizations for addressing cyber security and related risks to the insurance sector and the mitigation of such risks.

### 13.1 Classification of Critical Systems and Cyber Security Incidents:

Systems should be classified under categories based on criticality and Severity.

### 13.2 Organization's Cyber Resilience program

The varied challenges presented by cyber risk should be met with a broad response by insurers and Insurance Intermediaries. 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. In addition, a well-functioning cyber security management program consistent with cyber resilience best practices should be in place and verified through supervisory review. As described below, this level of response is consistent with the Insurance Core Principles.

To be effective, cyber security needs to be addressed at all levels of an institution. Generally, a cyber-security management program includes on-going process 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

It is generally recognized that best practices for cyber resilience should include but not limited to below key areas:

### 13.3 Identification

a. Identification means identifying critical assets, business functions and processes that should be protected against compromise.
b. Information assets (including sensitive personal information) and related system access should be part of the identification process.
c. Business process or Vendor risk should be identified and assessed as a part of on-

boarding and operations process.

d. Regular reviews and updates are key factors, as cyber risk is constantly evolving and "hidden risks" can emerge.

**13.4 Protection**

a. Controls should be in line with leading technical standards. Resilience can be provided by design. Comprehensive protection entails protecting interconnections and other means of access to insider and outsider threats. When designing protection, the "human factor" should be taken into consideration. Therefore, training is also an essential part of the safety net against cyber risk. Appropriate degree of IT controls shall be ensured for outsourced activities.

b. Availability factor of portals should be part of contracting and sourcing. Protection from DDoS Vectors needs to be part of sourcing and monitoring.

c. Appropriate access controls along with restriction based on least privileges roles should be part of application and access control design.

**13.5 Detection**

For critical systems cyber security monitoring is essential, as performing security events monitoring and or analytics would assist in detection and mitigation cyber incidents. These may include third party providers.

**13.6 Response and Recovery**

It is not always possible to detect or prevent cyber incidents before they happen, even with the best processes in place. For this reason, incident response planning is of great importance. Resumption of services (if interrupted) should be achieved within a reasonable timeframe, depending on the impact of the incidents and the criticality of the service. Contingency planning, design, and business integration as well as data integrity (also in the case of data sharing agreements) are key enablers for fast resumption. To make contingency planning effective, it is recommended to have a regular testing. Forensic readiness is essential to facilitate the investigations.

**13.7 Testing**

Testing programmes, vulnerability assessments and penetration tests are cornerstones in the testing phase. Testing should be included when systems are specified, developed, and integrated.

### 13.8 Situational Awareness

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

### 13.9 Learning and Reporting

Organizations should continually re-evaluate the effectiveness of Cyber security management. Lessons learned from cyber events and cyber incidents contribute to improved planning. New developments in technology should be monitored.

Cyber security incidents which are critically affecting the business operations and large number of customers should be reported to IRDAI within a Maximum period of 48 hours, upon knowledge.

Organizations must report information security incidents, where the confidentiality, integrity, or availability of critical information is potentially compromised, to the IRDAI and Cert-Fin with the required data elements, as well as any other available information, **within 48 hours** of being identified by the Organization's Information Security Team, Security Operations Center (SOC), or information technology department. In some cases, it may not be feasible to have complete and validated information prior to reporting. Organizations should provide their best estimate at the time of notification and report updated information as it becomes available

# 14. Platform/Infrastructure Security

**Objective:** Organization's IT infrastructure including servers, applications, and network and security devices shall be configured to ensure security, reliability and stability.

### 14.1 Secure Configuration Documents & Periodic Assessments

The configuration shall be based on Secure Configuration Documents (SCD). Organization shall develop baseline SCD based on OEM's recommendations and industry best practices. SCDs should be prepared for the following list (but not limited to) of components

- Operating Systems (Servers & End points – Laptop, Desktops)
- Web Server software (Tomcat, IIS, Apache HTTP, IBM HTTP and Oracle HTTP, etc.)
- Application Server software (Weblogic, etc.)
- Database Servers (Oracle, MS-SQL, MySQL, PostgreSQL,etc.)
- Network Components (Routers, Wireless Access Points, etc.)
- Security Devices (Firewalls, VPNs, IDS, IPS, etc.)
- Wireless

SCD should be reviewed for currency on a periodic basis by Information Security Team. The exceptions to configurations as recommended in SCDs owning to certain business requirements/limitations should be approved through formal exception process after adequate risk assessment.

The IT infrastructure should be subject to configuration review (vulnerability assessment/penetration tests) against defined SCDs on a periodic basis.

Regular scheduled assessments, such as internal and external vulnerability scans should be conducted for the IT Infrastructure including but not limited to software, applications, server, network, database, operating system, wireless devices, and other network equipment.
Frequency of conducting vulnerability assessment shall depend upon the criticality of the Information Asset (application, software, database, operating system, network devices and wireless networks). All Internet facing applications shall undergo vulnerability assessments before deployment in the production environment.

**14.2 Patch Management**

Organization's IT infrastructure should be updated with the supported, tested and reasonably latest OS and database patches including security patches and upgradation patches. Impact analysis and testing shall be performed for the recommended new patches, before deploying those in production environment. For the patches causing adverse impact or non-availability of business applications, exception approval documents should be maintained for future reference and audit purpose.

Patches for end-points may be tested in test environment before implementation on the user machines.

# 15. Network Security

Objective: The information transmitted across the Organization through its network shall be protected by deploying adequate network security controls.

**Policy, Procedures & Guidelines:**

a. Network shall be segmented into zones/subnets based on function and possibly location. Each of the zone/subnet may be further segregated into separate VLANs based on business and security requirements.
b. All network devices should be HARDENED based on their respective secure configuration documents before being deployed in production.
c. Logical position of firewall in network architecture should ensure that firewall is not bypassed. Defence-in-depth through placement of IDS/IPS solution shall be implemented to further control the internet traffic passing through these networks. These solutions shall be regularly updated with current signatures / characteristics of threats.
d. Remote access to organization's network resources over an un-trusted network (Internet/Extranet) shall be integrated into the overall network security management.
e. Clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.
f. Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control system of the business applications.
g. There should be segregation of duties for approval and implementation of configurations for network devices.
h. Adequate redundancy should be provided for network links and network devices. REDUNDANT NETWORK LINKS AND DEVICES SHOULD HAVE THE SAME LEVEL OF SECURITY AS THE PRIMARY LINKS. **All single points of failure within the organization network shall be identified and the risks in such a design shall be assessed**. Where possible, failover technologies shall be in place to address network failure. Network diagram (including wireless network) shall be documented and kept up to date.
i. Logs generated by critical network devices shall be collected and analyzed to identify threats and exceptions. Network security shall be monitored through a Security Operations Centre (SOC) to provide immediate response to threats.

# 16. Cryptography & Key Management

**Objective**: Organization shall protect the confidentiality, authenticity and integrity of information by cryptographic means wherever necessary. The level of protection applied using cryptographic keys shall be commensurate with the sensitivity and frequency of use of the information along with the environment where it resides/used.

**Policy, Procedures & Guidelines:**

**16.1 General directives on keys**

a. Digital signatures/certificates shall be acquired from the Certificate Authority (CA) licensed by the Controller of Certifying Authorities (CCA) India.
b. Accountability / responsibility for management of master keys shall be formally assigned within the organization in case of internal CA.
c. Key custodians must be made aware of their role and they shall formally acknowledge their obligations in administering the security of the keys.
d. Master keys for symmetric key/asymmetric key pair generation must be secured in a manner such that no one individual party is privy to the entire master key, wherever
e. applicable.
f. Keys/asymmetric key pairs shall be changed whenever a compromise occurs (or thought to occur), and whenever a party who is privy to a key/the private key component of the key pair, leaves the organization or changes role. A formal process must exist to revoke symmetric keys/asymmetric key pairs in a timely and effective manner. Revoked keys shall be destroyed.
g. Key backup process shall enable key recovery, but should not compromise key confidentiality and integrity. Request for recovery of keys/key pairs shall be made via a formal process that includes approval from competent authority.

**16.2 Retention of electronic keys**

a) Data encryption keys – symmetric/asymmetric keys used for encryption shall be available as long as any information protected (encrypted) by the keys needs to be decrypted.
b) Digital certificate verification – a public key shall be available as long as any information signed with the associated private key is maintained.
c) Master key used to derive other keys – master keys shall be available as long as there is a requirement to recreate derived keys in the future.
d) Keys used to generate hash algorithms – keys used to generate hash algorithms shall be available as long as there is a requirement to prove or otherwise the validity of a previously generated hash value.

# 17. Security Logging & Monitoring

**Objective:** Organizations shall establish logging and monitoring capabilities to detect security events in timely manner.

**Policy, Procedures & Guidelines**

**17.1 Logging & Monitoring**

a. Security logs shall be enabled on all critical information assets. A centralized approach to logging & monitoring (SOC set up) should be implemented.
b. Security Logs generated by different systems and devices shall be collected such that linking (correlating) events generated across these systems and devices is possible and should be maintained for a minimum period of six months and meet other specific regulatory stipulations as applicable.
c. Security logs shall be made available to the Law enforcement agencies, IRDAI and Cert-Fin as and when required.
d. Logging shall be enabled to track critical system activities which shall include:
    - User account management
    - Privileged user activities
    - Changes in OS configuration
    - Multiple authentication failures/simultaneous logins
    - Access to audit trail
e. All information systems including application, operating system, database, network and security devices shall maintain time synchronization with a standard time device/ server (NTP) to provide an accurate and traceable record of logged events.
f. Log Retention schedule should be compliant with Organization's record retention policy. All the logs and logging facilities should be protected against tampering and unauthorized access.
g. Monitoring reports should be published based on the management requirements. Periodic review of logs and monitoring reports for adequacy and contents should be performed.
h. Incidents reported should be closed within defined timelines.

## 18. Incident Management

Objective: To ensure information security and cyber security events and weaknesses associated with the information systems are communicated and corrective actions are taken in a timely manner.

i. Policy, Procedures and Guidelines for information security and cyber security incident management shall be prepared and implemented to discover, record, response, escalate and prevent information security events and weaknesses effectively.
ii. There should be a system in place to ensure information security events and weaknesses associated with the information assets are communicated and corrective actions are taken in a timely manner.
iii. An incident management process shall be established, documented, implemented and maintained by the organization. It shall include security Incident and weakness identification, reporting, recording, analysis, response, recovery and mitigation procedures. Roles and responsibilities of all the stakeholders of the incident management process shall be defined.
iv. Incident management team shall be established to take all incident related decisions. A communication channel shall be set up with internal parties and external organizations (e.g., regulator, media, law enforcement, customers).
v. Monitoring system should be in place so that proactive action is taken to avoid security incidents and malfunctions.
vi. The Information security and Cyber security incident classification criteria shall be documented. Security incidents shall be classified based on the criticality and severity.
vii. A process to assess the root cause of the incident and identifying the corrective and preventive measures shall be defined.
viii. For Incident and Cyber Crisis; a comprehensive cyber security response plan needs to be developed and referred.
ix. For Incident and Cyber Crisis; a comprehensive cyber crisis management plan (CCMP) needs to be developed and referred. The Organization will need to take effective measures to prevent cyber-attacks and to promptly detect any cyber-intrusions so as to respond / recover/ contain the fall out.
x. CERT-In/NCIIPC guidance may be referred by the organizations while formulating the CCMP.

**18.1 Incident Reporting & Escalation handling Processes & Procedures**

a. Deployment of suitable technology for incident reporting and guidelines and procedures for timely escalation and action incidents reported.

b. The logging, classification, diagnosis and rectification procedures for incident management shall be laid out in detail.

c. Incidents, classified as High or Critical, should be reported to CISO, CIO, CRO and other relevant stakeholders including CERT-in & CERT-Fin.

   I. Need for a knowledge base, which allows new incidents to be compared with logged and resolved incidents.

   II. Security incidents having noticeable impact on customer service, or requiring reporting of incidents to external entities, in terms of any legal, regulatory and / or statutory requirement should be reported only by the respective designated official.

**18.2 Review of the functioning of the preventive and detective controls**

a. The organizations are expected to be well prepared to face emerging cyber- threats such as ‘zero-day’ attacks, remote access threats, and targeted attacks.

b. The incident monitoring system should have a procedure to monitor, measure and review the effectiveness of the controls deployed.

# 19. Endpoint Security

Policy, Procedures & Guidelines: Policy, Standards, Procedures and Guidelines shall be developed to address the threats to endpoints in information system infrastructure and to prevent unauthorized access to endpoints.

### 19.1 Objective Endpoint Security

a. To ensure that endpoint has an updated (patched) operating system and anti-virus software has the latest virus definitions, etc.
b. To ensure system configurations are accurate and do not compromise the security requirements.
c. To prevent unauthorized external users and network traffic from gaining access to network.
d. To prevent unauthorized devices and other portable storage devices connecting to endpoint.
e. To prevent/detect any unauthorized software on the endpoints.
f. To address technical system and software vulnerabilities quickly and effectively.
g. Build capability to quarantine systems / devices if found to be non-compliant or infected.

### 19.2 Identity and access to end points

a. Endpoint device should be allowed to comply with Organization's "Acceptable Usage Policy" before allowing access to Organization's network.
b. User rights should be allocated based on the principle of least privilege in accordance with their business/functional requirements. User rights should be based on a "NEED TO HAVE" AND "NEED TO KNOW BASIS".

### 19.3 Network access control

Authentication mechanism for end points connecting from Organization WAN or external network shall be implemented to ensure entry of only authorized users.

### 19.4 Remote access

a. Organization should regularly review remote access approvals and revoke those that no longer have a compelling business justification
b. Organization should ensure appropriate and timely patching, updating and maintaining

all software on remote access devices

c. Encryption should be used to protect communications of critical data between the access device and the organization

d. VLANs, network segments, directories, and other techniques should be used to restrict remote access to authorized network areas and applications within the organization

e. While using TCP/IP Internet-based remote access, Organization needs to establish a VPN/Appropriate Communication channel over the Internet to securely communicate data packets over this public infrastructure.

**19.5 Application Control**

a. Organization can evaluate the likelihood associated with the threat agent, attack vector, and security weakness and combine it with an estimate of the technical and business impact to the Organization.

b. All endpoints/workstations owned by the organization shall be loaded with pre-approved licensed software. Any unauthorized installation of non-standard software on the workstation for personal or official use should be prohibited.

**19.6 Device control**

a. Appropriate controls shall be in place to control the risks arising out of usage of mobile storage devices such as USB's, CD-ROMs, RW-CD, external hard drives, cameras, portable media players, card readers, mobile phones etc.

b. IT Support team should configure all endpoint devices as per the baseline secure configuration documents provided by Information Security Team. Unlicensed or doubtful software/ applications should not be installed.

c. Whenever connecting to the LAN, it must be ensured that anti-virus agent is installed with latest signatures on the device.

d. Organization may consider to deploy security software like Data Loss Prevention (DLP) to identify, monitor and protect data in use, data in motion and data at rest.

# 20.Virtualization

Objective: To ensure protection of information during use of virtual environment within the IT infrastructure of the company.

Policy, Procedures & Guidelines: Approved Policy, Procedures & Guidelines for Virtualization of the systems shall be in place, which will detail, at least, the following:

- Centralized Administration of virtualized systems
- Provisioning and allocation of resources between different systems in virtualized machine
- Securing information resides in the host and virtualized machines

**20.1 Access Control**

a. Access Control shall be implemented and adequate process shall be in place to ensure no unauthorized virtual hosts or guests are created. Access from and to the host should be allowed through a firewall controls to restrict access to the necessary services only.
b. Network Access for the host OS should be restricted to management services and if required, to storage.
c. Administrative access for management of virtual networks, virtual servers and back up should be segregated.
d. Host OS to guest OS communications should be secured.
e. VMs should not be able to access or view the resources used by the kernel or host. These resources include storage and networks.
f. Access to virtual environment management console should be through centralized administrative console with audit logging capability.
g. If production and non – production VMs are hosted on the same host OS, adequate security controls should be in place to ensure logical segregation**.**

**20.2 Hardening of Operating Systems**

a. Appropriate hardening shall be implemented to prevent unauthorized file sharing, time synchronization.
b. All unnecessary programs shall be uninstalled, and all unnecessary services should be disabled.
c. Host OS must be patched regularly and in a timely fashion to ensure that the host OS is protecting the system itself and guest OSs properly. In addition, the same patching

requirements apply to the virtualization software.

d. VMs shall be configured by default to disable connections to peripheral devices. Connections to peripheral devices shall be approved.

**20.3 Partitioning and resource allocation**

Volumes or disk partitioning should be used and role-based access controls should be placed individually on each virtual machine.

**20.4 File Sharing**

File Sharing shall not be allowed between the host and the guest in order to keep the host OS files integrity.

**20.5 Back up**

Virtual systems shall need to be regularly backed-up for error recovery and continuity of operations.

**20.6 Monitoring**

Appropriate mechanism for monitoring the operations between the host and the guest should be put in place to ensure no unauthorized operations or no malicious operations or no resource monopoly happens between the VMs.

# 21. Cloud Security

Objective: To ensure that information processed, transmitted and stored on the cloud architecture is secure.

Policy, Procedures & Guidelines: Policy, Procedures & Guidelines shall be framed to provide direction for hosting the type of information, its criticality and the level of security controls to be adopted, on cloud or on any external hosting infrastructure

- With reference to the Electronic maintenance of core business records, records shall be hosted within India.
- The selection of cloud hosting model shall depend on the criticality of the information being hosted
- Wherever application/data/system hosting in a cloud is considered inevitable -for commercial, business, regulatory, legal or other reasons, approvals should be obtained by the organization from their respective senior management.
- Business justification for considering inevitable to host the data and system in Cloud. Classification of data to be hosted on Cloud Viz. Secret/Highly Confidential, Confidential, Public, Internal, etc.
- It should cover:
    - Security Control measures to be implemented by Cloud service provider/ Application Service Provider/Any Third-Party/Company for guarding against Data leakage / Data corruption /Security breach etc. as well as control measures in place to prevent, detect and react to breaches including data leakage
    - Due diligence process for selecting a suitable service provider

**21.1 Service Level Agreements**

a. An appropriate service level agreement shall be in place to address
    I. Sustainability, support for fail safe operations
    II. Data Retrieval time, protection of IPR, etc.
    III. Security control measures to prevent, detect and react to breaches including data leakage and demonstration of the same
    IV. Unilateral contract termination/exit clause
    V. Right to Audit for IRDAI /Law enforcement agencies and Cert-fin to access information / log
b. Service Provider's contract shall include clauses to ensure confidentiality, integrity,

availability and privacy of the data collected, processed, stored and disposed through cloud services.

c. Contracts with service provider shall include but not limited to following in addition to the other contractual requirement:
    i. SLA
    ii. Compliance to applicable laws & regulations
    iii. Data ownership
    iv. Authentication controls
    v. Log retrievals
    vi. Patch Management
    vii. Configuration Management
    viii. Application/System Security Testing
    ix. Data Recovery plan
    x. Data Deletion at separation or expiry of contract

**21.2 Cloud Access Control**

Appropriate Access control mechanism shall be implemented with reliable authentication mechanism to ensure

a. Data is not shared accidentally with other customers on the cloud
b. Cloud service provider/Application service provider/any third-party personnel controls are in place to provide a logical segregation of duties.
c. Logging and monitoring of privilege access shall be carried out

**21.3 Cloud Data Security**

a. Controls related to Operations Security shall be implemented for ensuring Secure Configuration, Application, OS, DB, Web Server, Back-up & Recovery, Change Management, Capacity & Demand Management, Protection against Malicious Code and Monitoring, Auditing & Logging security requirements on cloud.
b. D-in-transition cloud shall be in encrypted form, as appropriate to the information classification.
c. The Encryption techniques shall be implemented for cloud data hosting like Data in Transit and Data-at-rest for PII.
d. It is recommended to use appropriate Data Loss Prevention (DLP) solution to identify, monitor and protect sensitive data and manage the data risk for the organization.
e. Data retention and destruction schedules should be defined by the organization and service provider should be made responsible to destroy the data upon request, with special emphasis on destroying all data in all locations including slack in data structures

and on the media. The company should audit this practice, wherever applicable.

f. Data retention controls should also ensure that the multiple copies of the data stored in different locations are also destroyed post the retention timeframe.

# 22. Mobile Security

Objective: To ensure the security of information assets while tele-working and using the mobile devices by implementation of appropriate security measures to manage the risks associated with the usage of mobile computing devices and communication facilities**.**

Policy, Procedures & Guidelines:

Policy, Procedures and Guidelines shall be prepared and implemented to provide direction to the users of mobile computing so that corporate network remains secure.

The Policy, Procedures and Guidelines shall also cover:

a. Security measures for the organization's information processed using BYOD (Bring Your Own Device) and tele-working sites.
b. All employees, interns and externals using devices falling into the category "mobile devices" such as mobile phones, smart phones, portable devices, etc. shall acknowledge the security policy and the associated procedures & guidelines before they are allowed to use organization's network using mobile devices.

**22.1 Approved Devices/Services**

a. An inventory should be maintained of mobile devices in use, either owned by the organization devices or BYOD, associating owner name and identity for network access control shall be made mandatory. This inventory shall take into account at least but not limited to the list of identifiers such as device name, owner's ID, device serial number, device IMEI, device's MAC address, device capabilities, etc.
b. IT department of the organization shall prepare a list of authorized applications and shall have a documented process on management of such a list. This process shall cover the review mechanism for approved applications as well as approved devices/services on a periodic basis taking into account new devices/services available, new capabilities of devices and new threats.

**22.2 Incident Management:**

Appropriate authority shall be notified immediately on suspicion of a security incident, especially when a mobile device may have been lost or stolen

**22.3 Remote Blocking and Remote Wiping**

a. Remote device wiping or blocking mechanism for all devices accessing Organization's internal networks should be appropriately implemented to protect a data in case of

loss/theft of devices or change in employment status of staff member.

b. Controls should be in place to prevent devices from accessing the enterprise network if the devices have been rooted or jail-broken.

### 22.4 Network Access Control

a. Mobile Devices/Tele-working shall be allowed to connect to internal network to access corporate services with prior approval.

b. Appropriate secure authentication and authorization mechanism shall be put in place for providing access to the mobile devices/Tele-working into the organization's network. Wireless connectivity shall be permitted only with organization's approved encryption standards.

### 22.5 Mobile Data Security

a. Mobile devices containing confidential, personal, sensitive and generally all information belonging to company, except public information, shall employ encryption or equally strong measures to protect the corporate data stored on the device.

b. All mobile computing devices and all information assets used in tele-working, using corporate applications shall have anti-virus and/or anti-malware software installed and running.

# 23. Information System Audit

### 23.1 Eligibility & Selection of Auditor:

Independent Assurance Audit shall be carried out by qualified external systems Auditor holding certifications like CISA/ DISA/Cert-in empaneled Auditor.

### 23.2 Scope/Type Audit:

a. Scope of Audit shall include controls defined as per the annexure enclosed with this document.
b. Annual IS Audits should also cover branches on sample basis, with focus on large and medium branches, in critical areas like password controls, control of user ids, operating system security, anti-malware controls, maker-checker controls, Identity & Access management, physical security, review of exception reports/audit trails, BCP policy and testing etc.
c. This Assurance Audit shall be driven by the Information Security Team.

### 23.3 Frequency:

Audit shall be carried out for every financial year.

### 23.4 Executing IS Audit

During audit, auditors should obtain evidences, perform test procedures, appropriately document the findings, and conclude a report.

### 23.5 Reporting and Follow-up actions

a. There should be proper reporting of the findings of the auditors. For this purpose, each Organization should prepare a structured format.
b. The major deficiencies/aberrations noticed during audit should be highlighted in a special note and given immediately to the ISC and IT Department.
c. Minor irregularities pointed out by the auditors are to be rectified immediately.
d. Follow-up action on the audit reports should be given high priority and rectification should be done without any loss of time.
e. Audit reports need to be presented to the Risk Management Committee of the Board.
f. A copy of executive summary of the Audit report along with action taken note should be submitted to IRDAI within 30 days of completion of Audit

**23.6 Review**

Organization is advised to:

a. Review the selection and performance of auditor.
b. Ensure that the work of auditors is properly documented.
c. Be responsible for the follow-up on audit reports and the presentation of the quarterly review to the ISC.
d. Rotation of Auditors: Once in three years.

A Control Check List covering the domains specified in this report is provided in **Annexure A**

# 24. Legal References on Information and Cyber Security

This section may provide the organizations a broad idea about various statutory provisions available for Information and Cyber Security. An attempt has been made here to consolidate various legal provisions available on Information Technology, Cyber Security and Information Security for reference. While these consolidated provisions in **Annexure B** may be used for reference, the same may not be treated as exhaustive. The Organizations are requested to refer the relevant Act/regulation/rules/Amendments for updates/latest provisions.

**********

# Annexure B: Legal references for Information and Cyber Security

**Information and Cyber Security**

Cyberspace and cyber laws are emerging trends so far as the issue of legal jurisprudence is concerned. Unlike the traditional offline issues, which have developed and matured over a period of time; cyber laws, action and protection are at an evolving stage. Largely the basic principle of offline world would also apply in online world. However, given the intricacies of online world, there is definitely a need for special provisions of law and legal enforcement to deal with the issues of cyber space and virtual world.

The critical issues which revolve around with the legal aspects of transactions in cyber space would mainly evolve around the following:

- e- contracts and authentication
- e-signature and digital signature
- privacy and data protection
- Data retention and retrieval
- Electronic Evidence and admissibility
- Intermediary liability
- IP protection
- Dispute Resolution
- Jurisdiction and
- Cyber Crimes and enforcement

India's legislative framework to deal with the internet laws and online world is enshrined in the Information Technology Act, 2000 and Rules made there under. This was later amended by Information Technology (Amendment) Act 2008. It also leads to in the amendment in Indian Penal Code 1860, Indian Evidence Act 1872, the Bankers' Book Evidence Act, 1891 and the RBI Act, 1934 and related matters.

The IT Act and various Rules there under have provided the legal framework for storing, dissemination, processing and retrieval of electronic data. The Act also lays down guidelines and responsibility of conducting due diligence by body corporates and Insurance Intermediaries and adoption of reasonable security practices while handling information and data including sensitive personal data and information. There are also obligations entrusted for reporting of cyber security incidences to government authorities. Violation of these provisions can lead to

offences and penalties.

The definition of Information is quite wide under the IT Act and it means as under:

**“Information” includes** data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated microfiche”
The term Data as defined under IT Act means as under:

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

The term "Cyber Security" as defined under Section 2(nb) of the IT Act means
“protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction”.
Cyber Crimes can be classified into two broad categories:

**Computer Assisted Cyber Crimes:**
Spam, Phishing, identity theft, credit card fraud, Intellectual property violation on online space, pornography, unauthorized access are typical examples of Computer Assisted Cyber Crimes. Here computer is instrumental in committing the crime.

**Computer Oriented Cyber Crimes:**
Use of malicious software, Trojan, spyware, cyber terrorism, worm are typical examples of computer oriented cybercrimes. Here, the computer is the target of the crime.

**Protection of Personal Information and Reasonable Security Practice**
Bodies Corporate handling and dealing with personal information as well as dealing in online world are required to ensure that reasonable security practices and procedures are maintained. Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby

causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected.

"Reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

In this regard, the Government has notified The Information Technology (Reasonable Security Practice and Procedure and Sensitive Personal Data or Information) Rules 2011.

Pursuant to the above rules, Bodies corporate possessing, dealing or handling any sensitive personal data or information are required to observe following compliance requirements:

Key Obligations and Adherence

The following table lists out the key requirements and actionable for compliance of SPDI rules

| OBLIGATIONS | ACTIONABLE |
|---|---|
| **Policy for privacy and disclosure of information** | ❖ Provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information. The policy shall provide for:<br>• Clear and easily accessible statements of its practices and policies;<br>• type of personal or sensitive personal data or information collected;<br>• purpose of collection and usage of such information;<br>• disclosure of information including sensitive personal data or information;<br>• reasonable security practices and procedures<br>• Policy shall be published on website |
| **Collection of information** | ❖ Consent for collection should be obtained in writing. The information so collected should only be<br>• for a lawful purpose,<br>• considered necessary and |

| OBLIGATIONS | ACTIONABLE |
|---|---|
| | • connected with a function or activity of the body corporate or any person on its behalf.<br>❖ The provider of information at the same time should have<br>• knowledge of the fact that the information is being collected,<br>• the purpose for which the information is being collected,<br>• the intended recipients of the information,<br>• the name and address of the agency that is collecting the information, and<br>• the agency that will retain the information.<br>❖ The provider of information should be permitted to review the information so provided and to correct / amend if found inaccurate or deficient.<br>❖ Provider of information has an option<br>• Not to provide the data or information sought to be collected.<br>• option to withdraw its consent given earlier<br>• Such withdrawal of the consent shall be sent in writing to the body corporate.<br>❖ The Information not to be retained for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force. |
| **Disclosure of information** | ❖ Prior permission of the provider of information must be obtained in case of disclosure to any third party either in form of the contract or otherwise obtained specifically for disclosing the same.<br>❖ Such consent would be not be necessary in case of sharing with Government agencies or where such |

| OBLIGATIONS | ACTIONABLE |
|---|---|
| | disclosure is necessary for compliance of a legal obligation |
| Transfer of information | ❖ The following conditions must be satisfied while undertaking the transfer:<br>• The same level of data protection that is adhered to by the body corporate (transferor) is adhered to by the receiving party (transferee)<br>• it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information<br>• Such person has consented to data transfer. |
| Grievance handling | ❖ Body corporate to designate a Grievance Officer<br>❖ Publish his name and contact details on its website<br>❖ Grievances to be resolved within one month |
| **Reasonable security practices and procedures.** | ❖ Implement security practices and standards<br>• IS/ISO/IEC 27001<br>• Documentation of Practices and standards in the form of information security programme that contain<br>o managerial,<br>o technical,<br>o operational and physical security control measures<br>❖ the codes of best practices (by any industry association or an entity formed by such an association, whose members are self-regulating by following other than IS/ISO/IEC codes of best practices) for data protection.<br>❖ Such standard or the codes of best practices to be certified or audited at least once a year , through independent auditor, duly approved by the Central Government, or as and when there is a significant up gradation of its process and computer resource. |

**IT Service Provider's (IT intermediary) Liability**

In order to ensure the intermediary handling and processing information remain protected against the liability, they shall ensure adequate due diligence while handling third party information. Section 79 of the IT Act, 2000 provides for the liability of Insurance Intermediaries including internet service providers. Section 79 of the IT Act was amended by the IT (Amendment) Act 2008. Pursuant to the said amendment, an Intermediary shall not be liable for any third party information, data or communication link made available or hosted by them if:

- the function of the Intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored;
- the Intermediary does not initiate the transmission or select the receiver of the transmission, and select or modify the information contained in the transmission
- the Intermediary observes due diligence while discharging its duties and also observes such other guidelines as the Central Government may prescribe in this behalf.

It may be noted that the Intermediary shall lose the above immunity if the Intermediary is found to have conspired or abetted or aided or induced whether by threats or promise or otherwise in the commission of the unlawful act. Further, if the Intermediary upon receiving actual knowledge, or on being notified that any information, data or communication link residing in or connected to a computer resource controlled by the Intermediary is being used to commit the unlawful act, the Intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

**The Information Technology (Intermediaries guidelines) Rules, 2011**

The Central Government additionally has notified The Information Technology (Intermediaries guidelines) Rules, 2011 vide notification dated 11th April, 2011. These rules provide the guidelines and procedure to be dealt by Intermediaries as part of the due diligence and administration of takedown and procedural obligations by intermediaries.

| **Due diligence to the observed by intermediary** | **Actionable** |
|---|---|
| Publish the rules and regulations, privacy policy and user agreement for | Such rules and regulations, terms and conditions or user agreement shall inform the users of |

| Due diligence to the observed by intermediary | Actionable |
|---|---|
| access - or usage of the intermediary's computer resource by any person. | computer resource not to host, display, upload, modify, publish, transmit, update or share any information that:<br>• belongs to another person and to which the user does not have any right to;<br>• is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;<br>• harm minors in any way;<br>• infringes any patent, trademark, copyright or other proprietary rights;<br>• violates any law for the time being in force;<br>• deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;<br>• impersonate another person;<br>• contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource<br>threatens the unity, integrity, defence, 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 any other nation |
| Obligation on hosting/transmission | The Intermediary shall not 'knowingly' host or |

| Due diligence to the observed by intermediary | Actionable |
|---|---|
| | publish any information or *shall not initiate the transmission*, select the receiver of transmission, and select or modify the information contained in the transmission. |
| Take Down obligation | The Intermediary is required to disable such information that is in contravention of above, within 36 hrs. of knowing. Intermediary shall also preserve such information and associated records for at least ninety days for investigation purposes. |
| Right to terminate | The Intermediary shall have the right to immediately terminate the access or usage of the users to the computer resource of Intermediary in case of noncompliance with rules and regulations, user agreement and privacy policy. |
| Obligation to Report | The Intermediary shall be required to report cyber security incidents and also share cyber security incidents related information with the Indian Computer Emergency Response Team. |
| Obligation to Provide Information | The Intermediary shall provide information or offer assistance to Government Agencies for investigative, protective, cyber security activity. |
| Reasonable Measures | The Intermediary shall at times be required to have 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. |
| Grievance Officer | Intermediary is required to appoint a Grievance Officer and his contact details as well as |

| Due diligence to the observed by intermediary | Actionable |
|---|---|
| | mechanism by which any victim can notify their complaints. The Grievance Officer shall redress the complaints within one month from the date of receipt of complaint. |

The Indian Computer Emergency Response Team

The Government of India has notified The Information Technology (The Indian Computer Emergency Response Team and manner of performing functions and duties) Rules, 2013.

As per Rule 12 (1) (a) of IT (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 any individual, organization or corporate entity affected by cyber security incidents may report the incident to CERT-In. Service Providers, intermediaries, data centers and body corporate shall report the cyber security incidents to CERT- In within a reasonable time of occurrence on noticing the incident to have scope for timely action.

The following type of cyber security incidents shall be mandatorily reported to CERT-In as early as possible to leave scope of action.

- Targeted scanning/probing of critical networks/systems
- Compromise of critical systems/information
- Unauthorized access of IT systems/data
- Defacement of website or intrusion into a website and unauthorized changes such as inserting malicious codes, link to external websites etc.
- Malicious code attacks such as spreading of virus/worm/Trojan/Botnets/spyware
- Attacks on servers such as Database, Mail and DNS and network devices such as Routers
- Identity Theft, Spoofing and Phishing attacks
- Denial of Service (DOS) and Distributed Denial of Service (DDOS) attacks
- Attacks on Critical Infrastructure, SCADA Systems and Wireless networks
- Attacks on Applications such as E-Governance, E-Commerce etc.

Data Theft

Data theft involves issues of copyright violation, violation of privacy under IT Act 2000, as well criminal breach of trust and dishonest misappropriation under Indian Penal Code, 1860.

Section 43(b), read with Section 66 of the Information Technology Act 2000 and Section 379, 405 & 420 of Indian Penal Code deals with framework of data theft and penal provisions thereto.

Penalty and Compensation for damage to computer, computer system

Section 43 clearly provides for the provisions of damages by way of compensation against the person who without the permission of the owner or any other person who is in charge of a computer, computer system or computer network

(a) accesses or secures access to such computer, computer system or computer network or computer resource
(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer,
computer system or computer network;
(e) disrupts or causes disruption of any computer, computer system or computer network;
(f) denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;
(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under,
(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,
(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means
(j) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage.

**Confidentiality and Privacy**

Section 72A provides obligation to ensure confidentiality and privacy of electronic records or information to which any person has secured access. No such information/record can be disclosed without the consent of the person concerned, to any other person. Failure to maintain confidentiality and privacy shall make the person liable.

Similarly, Section 72A also provides obligation to person including intermediary who while providing the services has secured access under the terms of lawful contract to any material containing personal information about another person, discloses, without the consent of the person concerned, or in breach of a lawful contract, such person shall be liable.

**Penal Provisions**

The following chart captures the gist of penal provisions as applicable under the Information Technology Act 2000 dealing with the consequences of violations

**Adjudication Officer**

As per Section 46, the central government / state government can appoint an officer not below the rank of a Director to be an adjudication officer to hold enquiry in the matter with the power to decide if any person has committed any contravention of the Act or any rules, direction or order under the Act. The pecuniary jurisdiction is Rs 5 Crore.

**Cyber Appellant Tribunal**

The Government has constituted CAT to whom the appeals from the decisions of an AO may be preferred. Appeal against the decision of CAT can be made before the High Court.

**Penal Provisions**

The following chart captures the gist of penal provisions as applicable under the Information Technology Act 2000 dealing with the consequences of violations

| Section | Penalties |
|---|---|
| 43A (failure to protect data) | Damages by way of compensation to the person so affected.<br>• Upto Rs. 5 crore (adjudicating officer)<br>• Above Rs. 5 crore (civil court) |
| 65 (hacking / tampering) | imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both. |
| 66 (computer related offences) | Punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakhs or with both |
| 66B (dishonestly receiving stolen computer resource) | Punishable with imprisonment for a term of which may extend to three years or with fine which may extend to rupees one lakh or with both |
| 66C(identity theft) | Imprisonment for a term that may extend to three years and shall also be liable to fine which may extend to rupees one lakh. |
| 66E (Punishment for violation of privacy.) | imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both |
| 66F(cyber terrorism) | Imprisonment for life |
| 67C (Preservation and Retention of information by intermediaries) | imprisonment for a term which may extend to three years and shall also be liable to fine. |
| 71 (misrepresentation of material fact with Controller or the Certifying Authority) | Punished with imprisonment for a term which may extend to two years or with fine which may extend to Rs.1 lakh or with both |
| 72 (Breach of confidentiality and privacy) | imprisonment for a term which may extend to 2 years, or with fine which may extend to one lakh rupees, or with both. |
| 72A (Disclosure of information in breach of lawful contract) | Imprisonment for a term, which may extend to 3 years or with fine, which may extend to five lakh rupees, or with both. |

| Section | Penalties |
|---|---|
| 73 (publishing false electronic Signature Certificate) | punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both. |
| 74 (Publication for fraudulent purpose) | imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both |
| 85 (Offences by Companies) | every person who, at the time the contravention was committed, was in charge of, shall be guilty of the contravention. Where a contravention has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention |

| Act/Statute | Requirement | |
|---|---|---|
| Information Technology Act, 2000 (E-Governance Framework for Electronic Records and Electronic Signature) | • Authentication of Electronic Records & Electronic Signature (Sec. 3 & 3A) | • The authentication of electronic records should be done through digital signature in which case it should be using asymmetric crypto system and hash function using PKI infrastructure with a private key and a public key. This essentially include use of DSC for electronic signature.<br>• An authentication of electronic record can also be done by using a technique which is reliable and as specified in the second schedule of the Act. |
| | • Legal Recognition of electronic record and electronic signature (Sec. 4 & 5) | • Whenever law requires an information in writing such requirement shall be deemed to be satisfied if the information is rendered or made available in electronic form and accessible so as to be usable for a subsequent reference<br>• Whenever any law requires any information to be signed by a person then such requirement shall be deemed to be satisfied it is electronically signed. |
| | • Retention of Electronic Record and Audit of Documents (Sec. 7 &7A) | • Electronic records can be retained electronically when any law requires a document or information to be retained for a specified period. Audit of document preserved in |

| Act/Statute | Requirement | |
|---|---|---|
| | | electronic form, however no period for retention specified. |
| | • Validity of Contracts through electronic means (Sec. 10A) | • Contract established by way of proposals and acceptance in electronic form is enforceable |
| | • Attribution of electronic records, acknowledgement and time and place of dispatch of electronic records (Sec. 11, 12 & 13) | • Electronic record attributed to the originator in case it was sent by the originator or by authorized person or by an information system<br>• Acknowledgment of receipt takes places by originator in the form or method specified.<br>• Electronic record is dispatched at the time when it enters the computer resource outside the control of the originator.<br>• The time of receipt shall be based on the principle - the receipt occurs when the electronic record enters the designated computer in case specified. In other cases, the receipt occurs at the time electronic record is retrieved by the addressee. |
| | • Secure electronic record, electronic signature and security procedure (Sec 14, 15 & 16) | • Security procedure to be used in connection with the electronic record then such electronic record shall be considered as Secure |

| Act/Statute | Requirement | |
|---|---|---|
| Information Technology Act, 2000 (Penalties and Compensation and Offences) | • Damage to computer and computer system due to unauthorized access (Sec. 43)<br>• Failure to protect data compensation (Sec. 43A)<br>• Cyber Crime related offences (Sec. 65,66,67)<br>• Breach of Confidentiality and Privacy (Sec. 72)<br>• Punishment for disclosure of information and breach of lawful contract (Sec 72A)<br>• Offences by Companies (Sec 85) | Covered above |

| Act/Statute | Requirement | |
|---|---|---|
| The Information Technology (Reasonable Security Practice and Procedure and Sensitive Personal Data or Information) | • Procedure for collection, transfer, storing, disclosure & processing of sensitive personal data and information<br>• Implementation of reasonable security practices & code of best practices<br>• Certification/Audit on a regular basis through independent Auditor once in a year | Covered above |
| The Information Technology (Intermediary Guidelines) Rules, 2011 | • Due diligence by Intermediary and their liability<br>• Implementation of reasonable security practices by Intermediary<br>• Reporting of Cyber Security Incident to ICERT | • Covered above |

| | | |
|---|---|---|
| The Information Technology (Security Procedure) Rules, 2004 | • Requirements to be fulfilled to constitute a secure Digital Signature | • Rules for authentication of secure electronic records by means of secure digital signature.<br>• Public Key / Private Key/Smart card |
| The Information Technology ( Procedure and Safeguards for Interception, monitoring of Information) Rules 2009 | erception and decryption of information | Authorization to Govt. Agency to intercept, monitor or decrypt information generated, transmitted, received or stored in computer resources |
| Procedure for blocking of website | • Government notification dated February 27, 2003, G.S.R. 18(E) | • India (CERT-IND) shall be the single authority for issue of instructions in the context of blocking of websites. |
| The Telecom Unsolicited Commercial Communications Regulations, 2007<br>and<br>The Telecom Commercial Communications Customer Preference Regulations, 2010 | • Procedure for dealing with Unsolicited Commercial Communications and Obligations of access providers and tele marketers | • Privacy for numbers registered under DND.<br>• No call or SMS possible which are opted out<br>• 140 series number only to be used for telemarketing. |
| .IN Domain Name Dispute Resolution | • Procedure related to .in Internet Domain Names disputes | • types of disputes can be brought, and the criteria that will be considered by the arbitrators. |

| | | |
|---|---|---|
| Policy and Procedure (INDRP) | between registrar and complainant | • INDRP Rules of Procedure. These Rules describe how to file a complaint, how to respond to a complaint, the fees, communications, and the other procedures that will be used. |
| Insurance Act | • Regulation on Issuance of e-Insurance Policies<br>• Regulation on maintenance of Insurance Record | • Guidelines for issuance of policies in electronic form and also policy for maintaining insurance records including claims records in e- form.<br>• eiA to be maintained for issuance of e policies |
| Central KYC Record Registry | • File electronic copy of the clients KYC | • Enabling the central KYC through Central KYC<br>• Electronic copy to be uploaded in the central KYC |
| Indian Evidence Act, 1872 | Admission of electronic records | • Electronic record accepted as an evidence (Sec 3)<br>• Sec 65A & 65B Provides the procedures, standards for providing electronic evidence (Authenticity of records to be established as per the IT Act, 2000)<br>• Sec 85A, 85B, 85C & 88A provide the provision for presumptions regarding electronic agreements, electronic records & digital signatures/digital signature certificates<br>• Sec 34 and 35 provide for maintenance of records in electronic form |
| Companies Act, 2013 and rules | • Books of accounts and other relevant books maintained in | • Books of account allowed to be maintained in electronic form, |

| | | |
|---|---|---|
| made thereunder<br><br>Section 2(42), Companies Accounts Rules | electronic form shall remain accessible in India.<br>• Back up of the books of accounts maintained in electronic form including any place outside India, back-up should be kept on servers physically located in India on periodic basis | however adequate process and system available for its accessibility in India including for back-up in case records are kept outside India.<br>• In case books of accounts are maintained at other locations than the Required office location, the details of server to be provided to ROC |
| Trademark | • Protection against cyber squatting<br>• Infringement of trademark/Passing of Sec 135 TM Act<br>• ICANN domain name dispute resolution policy<br>• Meta tagging and hyper linking | • Legal remedies available for infringement and passing off<br>• Caution while linking of website etc.<br>• Relief can be obtained under ICANN in case<br>(i) respondent domain name is identical<br>(ii) respondent has no legitimate interest<br>(iii) respondent domain name was registered in bad faith<br>• IP risk to be assessed and appropriate strategy to be adopted to deal with IP infringement |
| Copyright Law | • Protection of data base | • Data bases are protected as literally work Sec 13 CA Act<br>• Software programmes can be protected under CA Act. Literary work includes computer programme Sec 2(1)(o)<br>• Reverse engineering permitted sec 51(1)(A)(c) of CA Act (for identification of identification of user) |

| | | |
|---|---|---|
| | | • Unauthorized access to data base punishable u/s43(b) of IT Act |
| Privacy and surveillance | • Inherently protected under article 21 of the Constitution i.e. right to privacy<br>• Reasonable surveillance permitted as per IT policy as defined<br>• Data protection and privacy also protected under IPC, 1860, Indian Contract Act, 1871, Specific Relief Act 1963 & Credit Information Companies (Regulation) Act, 2005 | National Cyber Policy 2013 has been framed with the following objectives<br>Creating a national level nodal agency that will co-ordinate all matters related to cyber security in the country<br>• Encourage organizations to develop their own security policies as per international best practices. The policy will ensure that all organizations earmark a specific budget to implement their security policies and initiatives and create an assurance framework,<br>• Certification of compliance to cyber security best practices, standards and guidelines<br>• legal framework will be created to address cyber security challenges arising out of technological developments in cyber space.<br>• 24X7 operational national level computer emergency response team (CERT-in) |
| Indian Penal Code 1860 – offences | • Forgery of Electronic Records Sec 463 & 468<br>• Making False Electronic Record Sec 464 | • Enabling provision on falsification of **electronic records** as provided under IPC |

| | | |
|---|---|---|
| | • Fabricating false in electronic records Sec 192<br>• Possession of Forged Electronic Record Sec 474 | • The relevant provisions of IT Act given effect in the enforcement law for trying of offences |

**********