Information Security Management Systems Policy

Information Security Framework for ISO 27001:2022

Table of Contents

Document Control

Document Name:	LUPIN LTD ISMS Manual – ISO 27001:2022
Abstract:	ISMS Manual describing Implementation framework of ISO/IEC 27001:2022
Document Reference:	ISO/IEC 27001:2022 Standard

Version History

Version	Date	Approved By	Changes & Reasons for Change
1.0	20 Nov 2014	Apex/ Steering Committee	Initial
1.1	13 Mar 2015	Apex/ Steering Committee	Changes: • Document put into the Kavach Template • Risk Ownership changed to 'Steering Committee' from 'Asset Owners' • Detailed Annexures have been removed and only their template retained for reference • ISO 27001 is replaced with ISO/IEC 27001:2013 • Provision for Documents of external origin has been added
2.0	12th Jan 2017	Apex/ Steering Committee	• Updated to include new locations in the certification scope.
3.0	10th Jan 2018	Apex/ Steering Committee	• Annual Review and revisited sections: 8.1.1, 11, 12, 17.2, 17.3, 17.4, 17.5, 18, 20, and 21
4.0	16th Apr 2019	Apex/ Steering Committee	• Detail understanding of the needs and expectation of interested parties • Addition of Kavach Templates • Risk and opportunities register added as annexure D • Elaboration of 'Planning of ISMS', 'management support' & 'operation planning and control'
4.1	17th Oct 2019	Apex/ Steering Committee	• Annual review – no change
5.0	8th Jan 2021	Apex/ Steering Committee	• Annual review – no change
6.0	6th Apr 2022	Steering Committee	• Addition of policy statements regarding continual improvement, technical compliance by VAPT and rollout of awareness training on annually • The purpose of the document is redefined • Addition of section 5.6, 6.3 in internal and external issues • Addition of section 17.7.3 in management review
6.0	28th Feb 2023	Apex/ Steering Committee	• Annual review – no change

Version	Date	Approved By	Changes & Reasons for Change
6.1	1st Aug 2023	Apex/ Steering Committee	• Added Aurangabad, Tarapur, Sikkim, Jammu, Dabhasa locations in section 4. Understanding the Organization and its context • Removed BKC and Kalina office from section 8.1.1 • Replaced Technical Security Officer (TSO) role with ISM in section 10.4 • Added Cloud Security Policy under Baseline Policies • Updated Kavach templates in section 12
7.0	13th Feb 2025	Apex/ Steering Committee	• Updated ISO 27001:2013 to ISO 27001:2022 in entire document. • Updated 7.1 and 9.1. • Added point 14.3. • Updated point 15.3.1. • Added 18.2.2. • Updated Authorization Table • Annual Review – Project Kavach Transition ISO 27001:2013 to ISO 27001:2022 • Reviewed and updated document as per ISO 27001-2022 and Added section 14.2.3 communication of objectives and 16.2 Creation and updating of documentation. • Added statements in Information Security Policy Statement section • Added some points in Internal and External Issues • Added some points in needs and expectation section • Updated ISMS Scope section • The Policies section updated policy name.

Authorization:

Prepared By	Reviewed By	Approved By
Name: Mr. Vaibhav Rathod Signature: Designation: ISM Date: 5th Feb 2025	Name: Mr. Sammit Potdar Signature: Designation: CISO Date: 11th Feb 2025	Name: Mr. KR Gupta Signature: Designation: Steering Committee (CISM) Date: 13th Feb 2025

Distribution List

Sr. No	Department or Function Name
1	Lupin Intranet “mylupinet.lupin.com”s

Lupin's Information Security Policy

At Lupin, we recognize information as a vital organizational asset and prioritize its security as a cornerstone of our operations. Protecting confidentiality, integrity, and availability of information is essential for achieving our business objectives.

We have implemented an Information Security Management System (ISMS) framework that includes robust policies, procedures, and technology solutions. Information assets are classified by their business value and risk exposure to ensure optimal protection. Compliance with applicable data protection laws and regulations for sensitive and Personally Identifiable Information (PII) is non-negotiable.

Every Lupin team member plays a crucial role in safeguarding information by adhering to security practices, participating in regular awareness training, and maintaining compliance with our policy. The Information Security Steering Committee oversees ISMS implementation, driving continuous improvement, periodic vulnerability assessments, and operational excellence.

Through proactive resource allocation for training and technology investments, Lupin reaffirms its commitment to secure business processes and systems while fostering a culture of accountability.

Together, we uphold the shared responsibility of protecting information, ensuring sustainable growth and success for the organization.

Signed
Nilesh Deshbandhu Gupta

Digitally signed by Nilesh Deshbandhu Gupta
DN: c=IN, o=Personal, title=6932, pseudonym=805qvc7g2JocHz436d9naexrfybmwt, 2.5.4.20=109981f538c9b5977dbe12906d79bec1952a6256119ccb991416d6372ec44b31, postalCode=400049, st=Maharashtra, serialNumber=7a16dcea8b43492f4add09114ed80d4fed841982fa49f5cee0c8f5c83172792c, cn=Nilesh Deshbandhu Gupta
Date: 2025.04.16 16:41:54 +05'30'

Nilesh Gupta
Managing Director

1. Purpose

This document is intended to provide guidance for Lupin's employees (and contractual workers), external/internal auditors to effectively establish and sustain the Information Security framework in the Organization and implement the activities related to Information Security Management Systems (ISMS) clauses 4 to 10 as listed in ISO/IEC 27001:2022 Standard.

2. Reference

This document shall refer to Information Security Management System Policies and Procedures and wherever any other Lupin organizational document is required.

3 Definition

The definitions used in this document are as adopted in Information Security Management System Policies and Procedures. Additional explanations are written wherever required. In case of conflict definitions as included in ISO 27001 shall prevail.

4 Understanding the organization and its context

Lupin has established, implemented, and maintained processes to understand the context of the organization, including both internal and external issues that are relevant to its information security management system (ISMS). These processes also include the identification of the needs and expectations of interested parties and determining the scope of the ISMS defined in ISMS Scope document.

4.1 Lupin understands the sensitivity of its business and wishes to ensure compliance to all legal and regulatory requirements in addition to meeting its organization's mission.

4.2 Lupin has identified the internal and external issues that can affect its ISMS objectives. These issues include but are not limited to the following:

5 Internal Issues:

5.1 Information security breaches affecting confidentiality, integrity and availability of information and information assets –

a) Insider Threat
b) Organizational culture including lack of awareness
c) Weak/ ineffective internal controls
d) Risk appetite
e) ISMS Roles and responsibilities not properly assigned
f) Unavailable resources
g) Remote working environment
h) Change in technology
i) Data and Intellectual property protection Handling of PHI/PII Data

6 External Issues:

6.1 Non-compliance to legal, regulatory and contractual requirements
6.2 Political and economic conditions
6.3 Dynamic Changes in the business environment
6.4 Market Conditions and competition
6.5 Third party (vendors, customers, service providers) information security risks
6.6 Cyber Threats
6.7 Cross border data protection concerns due to varying regulations.
6.8 Pandemics and Health Crises

For organization structure, please refer to the Information Security Organization Policy and Procedure.

7 Understanding the needs and expectations of interested parties

7.1 Lupin's business is supported by Information Security infrastructure and IT is an enabler for achieving the intended organization's Information Security objectives. The following are identified as the interested parties which are relevant for the Lupin Information Security Management system.

Relevant Interested Parties	Classification	7.1 b) and c) Requirements of these parties
Lupin Share Holders	Internal	• Check and balance on Information Security spending and Objective • Security of investment
Lupin Board of Management	Internal	• Assurance that all Information Security Risks are identified and mitigated to accepted Risk level • Minimal disruptions to business • Adherence to legal, regulatory and contractual requirements
End Users (Patients)	External	• The information and test reports published by Lupin are reliable and authentic • Lupin protects all personal health information (PHI) and patient reports
Bulk Customers	External	• ICT role in supply chain has been identified and made reliable to meet its contractual obligations
Regulators	External	• Lupin meets all regulatory requirements for security of all kinds of information it holds • Security breaches and incidents to be reported immediately.
Employees	Internal	• Lupin protects all relevant information of its employees • Skill enhancement through training and skill development program
Vendors	External	• Lupin shall enforce and meet the information Security with its vendor's information and know-how. • Adherence to legal, regulatory and contractual requirements

Relevant Interested Parties	Classification	7.1 b) and c) Requirements of these parties
Auditors	External	• Access to accurate and up-to-date documentation related to information security controls • Security of the organization's data based on Information security pillars of Confidentiality, Integrity & Availability
Certification Bodies and External Auditors	External	• Management's commitment to promote any standard • Business needs and client requirements for best practices • Understanding of the best practices by the employees • Continuous Improvement • Management directions, roles and responsibilities • Compliance with applicable standard(s) that the Lupin is registered to. • Compliance with any applicable legal or other requirements that Lupin has obligations for.

8 Scope of ISMS

The Information Security Management System (ISMS) of Lupin is implemented as per ISO 27001-2022.The detailed scope, including covered locations and functions is defined in the "*ISMS Scope Document*"

9 Information Security Management System

9.1 Lupin has implemented Information Security Management systems (ISMS) and has internally branded as Kavach (India) and SHIELD Global)

9.2 Lupin's information systems contain data that is fundamental for its daily operations and effective service provision. Hence, Lupin has designed and implemented adequate security policies, procedures and controls to protect confidentiality, maintain integrity, and ensure availability of all information stored, processed and transmitted through its information systems.

9.3 Given the critical and competitive nature of the business of Lupin, protection of its information assets should be commensurate with its business value and risk.

9.4 The Information Security Framework of Lupin through the elements as explained herewith seeks to express the intent of Lupin and the required action it shall need to take, in order to effectively establish, maintain and sustain the Information Security paradigm in the Organization.

9.5 The purpose of this framework is also to ensure that due care is exercised in protecting the computing systems and related information assets of Lupin. "Due care" is defined as the cost-effective protection of information at a level appropriate to its value.

9.6 Information, regardless of its source and nature, is an asset for Lupin. Its accuracy, availability, confidentiality, authenticity, integrity and reliability are essential to business to allow both confidence in customers and the decisions which are based upon it and to engender good relationships with business associates and company representatives.

9.7 Lupin ensures that Information Assets; which includes, computing systems, network infrastructure equipment, software, applications, databases, and services offered by the Organization through its network infrastructure comprising of NTUs (Network Terminating Units), routers, switches, hubs, assets in paper and other media which are utilized by the employees while discharging their duties, is protected from inappropriate access, disclosure, modification, or damage, thereby ensuring that Confidentiality, Integrity, Availability is maintained and sustained.

9.8 Also safeguarding of supporting utilities like electrical supply, air-conditioning, (UPS) Uninterrupted Power Supply Systems, fire safety systems, cabling in premises, are also called as Information assets as they contribute in maintaining the continuity of business operations and maintaining the creation /transmission /storage /usage /processing /sharing /destruction of information within Lupin and its business associates and customers.

10 Leadership

Lupin's Top management demonstrates leadership and commitment by ensuring the integration of the ISMS into the organization's overall governance framework, ensuring sufficient resources, and providing direction on information security risk management.

10.1 Lupin leadership has been the guiding factor and great support to Information Security.

10.2 An APEX Committee (hereafter may be referred to at APEX) for Kavach & SHIELD, reviews the ISMS activities at organizational level. The committee is chaired by MD and has senior members from verticals associated with information security.

10.3 For the purpose ISO/IEC 27001:2022 APEX has nominated a steering committee comprising Lupin CIO, CISO, CISM and senior representative from Legal and HR.

10.4 The Lupin Information Security Council consists of an Information Security Officer (ISO), Chief Security Officer (CSO) and Information Security Manager (ISM) responsible for execution of ISO/IEC 27001:2022 requirements.

11 Leadership Commitment

11.1 Information Security Policies (Refer 12) and ANNEX B Statement of Applicability are established, and information security objectives (Refer ANNEX A) are clearly defined. The policies and information security objectives are in alignment with Lupin's strategic direction.

11.2 Information Security management system is well integrated with organization process. The ISMS refer to other standards and process documents wherever relevant.

11.3 APEX has approved the Information Security Organization Policy for resources. Operations resources with required competencies are made available.

11.4 Lupin's Management ensures proper communication, charting out importance of ISMS for Lupin and following the requirements as laid down in policies.

11.5 Lupin's Management reviews the ISMS for its purpose, objective and effectiveness. Reviews of ISMS policies, processes and reports are conducted on a periodic basis and approved by the management. The effectiveness of the ISMS machinery is evaluated through measurable metrics and reviewed by the management (APEX) on a half yearly basis. Refer *KPI Review metrics*- Lupin document.

11.6 Lupin's management provides relevant directions and support wherever required.

11.7 Lupin's management ensures continual improvement by ensuring action on audit points, defining new objectives and taking on new technological projects.

11.8 Lupin's management supports relevant leadership roles in demonstrating their commitment to information security by ensuring they take responsibility for implementing and upholding security measures within their respective areas.

12 Policies

12.1 The following set of Policies called APEX policies has been approved by APEX committee to make sure that it is appropriate, includes framework for setting ISMS objectives, shows management commitment to satisfy applicable requirements, and ensures continual improvement.

APEX policies:

12.1.1 ISMS Scope Applicability_Lupin_v2.0
12.1.2 Information Security Management System Policy_Lupin_v7.0
12.1.3 Information Security Organization Policy and Procedure_Lupin_v8.0
12.1.4 Information Classification Policy and Procedure_Lupin_v12
12.1.5 Information Risk Assessment & Treatment Policy and Procedure_Lupin_v12.0
12.1.6 Information Security Sustenance Policy and Procedure_Lupin_v7.0

Annexures of Information Security Management System Policy:

Annex A - ISMS Objective_Lupin_V9.0
Annex B – ISMS SOA Lupin_V 8.0
Annex C - Communication Plan Lupin_V8.0
Annex D - Interested Parties, Risks & opportunities register_V4.0
Annex E – Information Security Internal Audit Procedure_v1.0
Annex F - Management Review Procedure_v1.0

There are also Baseline policies and IT Security Policies as follows:

BASELINE Policies:

12.1.7 Acceptable Usage Policy_Lupin_V9.0
12.1.8 Cloud Security Policy_v2.0
12.1.9 Compliance Policy_Lupin_v8.0
12.1.10 Human Resource Security Policy and Procedures_Lupin_v8.0
12.1.11 Incident Management Policy and Procedure_Lupin_v10
12.1.12 Kavach Applicable legislation.v.2.0
12.1.13 Outsourced Services Security Policy and Procedure_Lupin_v8.0
12.1.14 Physical Security Policy_Lupin_v8.0

IT Security Policies:

12.1.15 IT Security Policy_Lupin_v8.0
12.1.16 BYOD Policy Procedure_Lupin_v7.0
12.1.17 Equipment Security Policy_Lupin_v9.0
12.1.18 Compliance to CERT-IN Guidelines_v2.0

ANNEXURES OF IT SECURITY policies:

12.1.19 Access Control Policy_Lupin_v7.0
12.1.20 Asset Management Policy.v.2.0
12.1.21 Backup Restoration and Media handling Policy_Lupin_v7.0
12.1.22 Change Management Policy_Lupin_v8.0
12.1.23 Configuration Management Procedure_Lupin_v1.0
12.1.24 Email Security Policy_Lupin_v8.0
12.1.25 Malicious Code Security Policy_Lupin_v8.0
12.1.26 Operations and Communication Management Policy_Lupin_v7.0
12.1.27 Password Security Policy_Lupin_v9.0

Kavach Templates:

12.1.28 KPI Review Metrics_Lupin_v8.0
12.1.29 RARTP Template_Lupin_v9.0
12.1.30 ICS Template_Lupin_v9.0
12.1.31 3p List Template_Lupin_v5.0
12.1.32 Incident Management Register Template_Lupin_v6.0
12.1.33 Incident Report Template-Lupin-V7.0
12.1.34 Kavach Performance Ratings Template_Lupin_v7.0
12.1.35 HOD DR Meeting Sample MOM_Lupin_v.5.0
12.1.36 CACA Template_Lupin_v6.0
12.1.37 Third Party Security Risk Assessment Questionnaire_Lupin_v2.0
12.1.38 Competency Matrix_Lupin_v1.0
12.1.39 DR List Template _Lupin_5.0
12.1.40 Risk Recognition Form_Lupin_v.5.0
12.1.41 Participant Attendance Template_Lupin_v5.0

12.2 The information security policies are in line with the strategic direction of Lupin's management. They are reviewed and updated once a year and/or when a major change is required.

12.3 The main objectives of the information security policies are:

12.3.1 To ensure confidentiality, integrity and availability of information and information assets

12.3.2 To ensure a strong authentication, authorization and auditability mechanisms are in place so that information is available on a need-to-know basis

12.3.3 To ensure implementation and sustenance of information security awareness in the organization.

12.3.4 To ensure continual improvement of all controls and capabilities pertaining to information security.

12.3.5 To ensure compliance to all applicable legal, regulatory and contractual obligations for information security.

12.4 The information security policies are documented and made available on the intranet portal for all employees and are also communicated to other interested parties as appropriate.

13 Organizational roles, responsibilities and authorities

Lupin has defined the roles, responsibilities and authorities in Lupin *Information Security Organization Policy and Procedure*. Performance of responsibilities and authorities is reported to relevant top management in the form of metrics and reports.

14 Planning

Lupin has defined and documented its approach to managing risks and opportunities that may affect the achievement of information security objectives, in accordance with the organization's strategic direction.

14.1 Addressing Risk and Opportunities:

14.1.1 General Requirements:

Lupin has planned its Information Security Management System in the form of Kavach Program. Kavach is a program which includes many Information Security Projects and plans. Lupin ensures that each information security project achieves its intended outcome, prevents or reduces any undesired effects and supports the achievement of overall continual improvement.
Refer Annexure D - Risks & Opportunities register.

14.1.2 Information Security Risk Assessment:

Lupin has adopted a comprehensive Risk assessment methodology. The process-based methodology complies with the requirements of ISO 27005 and ISO 31000 risk management standards. The process of Risk Assessment is documented in *Information Risk Assessment and Treatment Policy and Procedure*. The result is documented in the Risk Assessment as part of the overall Risk Assessment and Risk Treatment Sheet. Lupin also ensures that Risk is owned by the 'Steering Committee' as they have authority and influence over Risk.

14.1.3 Information Security Risk Treatment:

Lupin compares the result of Information Security Risk obtained as a result of Risk Assessment exercise and decides if it must be treated or acted upon as an opportunity. The Process of Risk treatment is documented in Information *Risk Assessment and Treatment Policy and Procedure,* and the result of risk treatment is documented in *Risk Assessment and Risk Treatment Sheet*. The control required to mitigate are documented and presented for approval to management. Once approved, an action plan is charted for their implementation. A Statement of Applicability (Refer Annexure B) with reference to ISO/ISC 27001:2022 Annexure - list of controls - is prepared to check if any relevant controls are missing.

Lupin ensures that SMART (Specific, Measurable, Achievable, Realistic and Time-bound) objectives are drawn for Information Security. The Information Security objectives are reviewed and changed when required and are consistent with the information security policies and consider the applicable requirements and risk management results.

14.1.4 Measurable function level objectives have been defined and aligned to information security objectives. Refer Annex A – Function level ISMS objectives Lupin.

14.1.5 Information Security Objectives are communicated to relevant stakeholders to ensure awareness and commitment at all levels within Lupin.

14.1.6 Lupin also ensures that plans to achieve the information security objectives shall identify action, resources, responsibility, timelines and metrics for measurement. (Refer Annex A – Function level ISMS objectives Lupin and KPI review metrics sheets).

14.2 Planning for Changes:

14.2.1 Lupin ensures that the changes made to the information security management system are carried out in a planned manner.

15 Support

15.1 Resources

15.1.1 Lupin has ensured that adequate resources, which include infrastructure, information and people, are available for implementation, maintenance and continual improvement of ISMS in the organization.

15.2 Competency

15.2.1 Lupin ensures that resources required have relevant competency such as appropriate education, training and experience to perform their assigned roles. In the organization, if any designation has been included, the competency requirement created by HR (or Talent Management) and the manager shall be considered as enough. Competency for operation processes shall be defined and documented by respective managers in consultation with HR/SMEs.

15.2.2 To attain the necessary competence, Lupin hires/ contracts competent people or provides training to employees for skill enhancement as per their roles and responsibilities.

15.3 Training and Awareness

15.3.1 Lupin ensures that all personnel in Lupin including Employees, Contractors, Suppliers, and Third Parties are made aware about the Lupin Information Security Policies and Procedures, Acceptable Usage for their roles and responsibilities and disciplinary action in case of violations. Personnel shall be made aware of their contribution to the effectiveness of the information security management system, including benefits of improved information security performance. Various modes of awareness including classroom sessions, online training modules and other communications may be used to achieve the objective of security awareness. Effectiveness of awareness programs for employees are evaluated through e-module quizzes and/ or classroom interactions. Awareness programs shall be conducted at least once in a year.

15.4 Communication

15.4.1 Lupin has maintained a communication plan which includes what to communicate, when to communicate, with whom to communicate, who shall communicate and what shall be the mode of communication.

Refer Annexure C – Communication Plan

16 Documented Information

16.1 General

16.1.1 Lupin has identified all documented information for ISO/IEC 27001:2022 standard and any other legal or contractual requirements for the effectiveness of ISMS.

16.2 Creation and Updating

16.2.1 All ISMS documents/records are created, reviewed, and updated in a controlled manner. All documents:

- Clearly identify and describe title, date, version and author.
- Reviewed and approved for adequacy by authorized personnel.

16.3 Control of Documented information

16.3.1 All ISMS related documents/Records are protected & controlled. The protection & control is aimed at ensuring availability of the latest updated, released and in-force policies and procedures for use.

16.3.2 Lupin ensures that documented information is available to authorized persons when required, is adequately protected from loss of Confidentiality, Integrity, availability and is subject to improper use. This has been achieved by putting controls on distribution, Access, Retrieval, Use, Storage and Preservation, Changes, Retention and Disposition. (Refer to Information Asset Classification Policy and Procedure.)

16.3.3 The documents created are classified and labelled clearly to identify the document, the creator, reviewer/approver, the version number, date and description.

16.3.4 The documents/records are being reviewed on a periodic basis and the review details are captured of the same.

16.3.5 Documents of external origin where the controls are not possible are treated as internal documents.

17 Operation

Lupin has established and implements processes for the treatment of information security risks in line with the determined risk treatment plan and has integrated these into its operational procedures.

17.1 Operation Planning and control

17.1.1 Lupin plans and implements controls to meet the information security requirements as per ISMS objectives and the ISO 27001:2022 standard.

17.1.2 Lupin maintains information in the form of documents and records to support its information security functions. Such information is retained as per requirements of the Acceptable Usage Policy and Information Classification policy.

17.1.3 Any planned or unplanned changes are dealt with as per the change management policy of Lupin.

17.1.4 Outsourced processes of Lupin are identified and documented in the 3p List of Lupin.

17.2 Information Security Risk Assessment

17.2.1 Please refer to *the Information Security Risk Assessment and Treatment Policy and Procedure* and *Risk Assessment and Risk Treatment Sheet*.

17.3 Information Security Risk Treatment

17.3.1 Please refer to the Information Security *Risk Assessment and Treatment Policy and Procedure and Risk Assessment and Risk Treatment Sheet*.

18 Performance Evaluation

18.1 Performance Evaluations

18.1.1 Lupin ensures that ISMS performance is evaluated on defined intervals and on management directives. (Refer *Kavach Performance Ratings Template*-Lupin)

18.2 Monitoring, measurement, analysis and evaluation

18.2.1 Lupin develops various metrics to ensure the effectiveness of applied controls and overall effectiveness of ISMS. Metrics consist of parameters to be measured, methods and units for monitoring, measurements, analysis and evaluation, frequency, responsibility and reporting of metrics. (Refer *KPI Review Metrics Template*-Lupin)

18.2.2 Lupin has identified relevant personnel for analyzing and evaluating the results of KPI Review Metrics.

18.3 Internal Audits

18.3.1 Lupin ensures that internal audits are performed at regular intervals and should conform to ISO/IEC 27001:2022 standard and other identified and defined organizational requirements.

18.3.2 Lupin ensures that Audit criteria and scope are well defined, Auditors competency is matched, results of audits are reported to management and documented information relevant to audit process is kept. (Refer *Lupin Kavach Sustenance Policy and Procedure*)

19 Management Reviews

19.1 Lupin ensures that management review happens at least once every year. The Steering committee/ Apex Committee reviews ISO 27001 sustenance activities to ensure its continuing suitability, adequacy and effectiveness. The management review includes:

a) Action from previous reviews
b) Changes in external and internal issues as mentioned in 5 and 6
c) Feedback on information security performance.
d) Status of nonconformities and corrective actions
e) Input from Monitoring and measurement results
f) Inputs from internal and external audits
g) Inputs from Information Security Objective fulfilments
h) Feedback from interested parties
i) Result of Risk assessment and Risk treatment
j) Opportunities for Continual improvement

a

19.2 The management upon review suggests way forward, decisions or actions in the form of:

a) Improvement in the effectiveness of the ISMS.
b) Modifications of existing procedures that affect information security, as necessary, to respond to internal or external events that may have an impact on the ISMS.
c) Resources needed to manage or implement the ISMS.

19.3 The review proceedings are documented in the form of minutes and circulated to all attendees.

20 Improvements

Lupin is committed to the continual improvement of the ISMS by addressing nonconformities, taking corrective actions, and making necessary adjustments based on performance evaluations and changes in the risk environment.

20.1 Continual Improvement

Lupin continually improves the suitability, adequacy and effectiveness of the information security management system.

20.2 Nonconformity and corrective actions

20.1.1 Lupin ensures that all nonconformity observed are immediately be reacted to either by correction or dealing with the consequences of such non-conformity.

20.1.2 An evaluation is conducted to eliminate the cause of nonconformity by reviewing the nonconformity, doing root cause analysis and determining if similar non-conformity exists or has potential to occur.

20.1.3 Lupin implements any action needed, review the effectiveness of correction and if necessary, make changes.

20.1.4 The Corrections and corrective actions are documented, recorded in CACA template of Lupin and retained.

21 Annexures

Annex A - ISMS Objective_Lupin_V9.0
Annex B – ISMS SOA_Lupin_V 8.0
Annex C - Communication Plan Lupin_V8.0
Annex D - Interested Parties, Risks & opportunities register_V4.0
Annex E – Information Security Internal Audit Procedure_v1.0
Annex F - Management Review Procedure_v1.0

The Steering Committee meeting is attended by steering committee members and is conducted by the ISM along with ISO and CSO.

a) CISM shall chair the meeting
b) During absence of CISM, one of the members from the nominated steering committee shall choose a chairperson among themselves for that meeting only.
c) ISO shall be the coordinator of the meeting and communicate the agenda in advance and circulate minutes of the meeting after the completion of meeting.

22 Disclaimer

22.1 Lupin reserves all rights and is the exclusive owner of all intellectual property rights over this information security policy and procedure document. This information security policy and procedure document shall not, either in part or in full, be reproduced, published, copied, displayed, distributed, transferred, stored into any media (such as floppy diskettes, hard disks, USB Drives, Pen Drives, Memory Cards, CDS, DVD's), and/or captured or transmitted through by any means (electronic, digital, mechanical, photocopying, recordings, video and film or photographs and otherwise) by any person without prior written consent from the Information Security Team of Lupin. The information security policy and procedure document are meant to be published on the intranet of Lupin and/or any other forum as decided by the management of Lupin. Anything not specifically stated in this information security policy and procedure document shall not be considered as implied in any manner.

22.2 For any clarifications related to this information security policy and procedure document with respect to its interpretation, applicability and implementation, please write to kavach@lupin.com/shield@lupin.com