# MOREPEN LABORATORIES LIMITED

CIN: L24231HP1984PLC006028

**Registered Office:** Village Morepen, Nalagarh Road, Near Baddi Distt. Solan, Himachal Pradesh–173 205
Email: plants@morepen.com, Website: www.morepen.com,
Tel.: +91-1795-266401-03, 244590, Fax: +91-1795-244591

**Corporate Office:** 2nd Floor, Tower C, DLF Cyber Park, Udyog Vihar-III, Sector-20, Gurugram, Haryana-1221016; Email: corporate@morepen.com, Website: www.morepen.com,
Tel.: +91-124-4892000

# INFORMATION SECURITY POLICY

# Contents

## 1. Executive Summary

1.1 This document, the Morepen Laboratories Limited Information Security Policy (Here after referred to as "Morepen Laboratories Limited -ISP"), is written with the intent of highlighting various policies with respect to information security and business requirements. The Morepen Laboratories Limited -ISP is a part of the overall management system based on the business risk approach to establish, implement, operate, monitor, review, maintain and improve information security at Morepen Laboratories Limited

## 2. Introduction

2.1 Morepen Laboratories Limited is engaged in a comprehensive range of activities within the pharmaceutical and healthcare sectors, focusing on the production and distribution of APIs (Active Pharmaceutical Ingredients), formulations, diagnostic devices, and OTC (Over The Counter) products, along with providing contract manufacturing services and R&D.

## 3. Scope

3.1 This policy applies to all employees, consultants, vendor staffs, trainees, and other personnel working for Morepen Laboratories Limited in physically or virtually from any location approved by Morepen Laboratories Limited.

## 4. Information Security Objective.

4.1 To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations

4.2 Information is protected from unauthorized access, use, disclosure, modification, disposal or impairment, whether intentional or unintentional, through appropriate technical and security measures;

4.3 The Confidentiality, Authenticity, Integrity and Availability of all such information, whether acquired permanently or in transit, provided or created, is ensured at all time;

4.4 Any security incidents, security weakness and infringement of the policy, actual or suspected, are reported, investigated and appropriate corrective are initiated;

4.5 Awareness programs on Information Security are available to all employees and wherever applicable to third parties via, subcontractors, consultants, trainees, vendors etc. and regular training is imparted to them; and

4.6 All legal, contractual and regulatory requirements with regard to information security are met wherever applicable.

## 5. Management Commitment to Information Security

5.1 At Morepen Laboratories Limited the management shall commit to the requirements of establishing ISMS as per the following:

5.1.1 To establish and provide the intent of Morepen Laboratories Limited's management support ensuring that the business requirements are met in secure manner.

5.1.2 Ensuring the integration of the information security management system requirements into the organization's processes.

5.1.3 Morepen Laboratories Limited -ISP shall be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended users;

5.1.4 Organization to develop and maintain an effective Information Security Management System (ISMS) consisting of an IS policy and supporting procedures

5.1.5 Ensuring the integration of the ISMS requirements into Morepen Laboratories Limited's processes.

5.1.6 Ensuring that the resources needed for the information security management system are available.

5.1.7 Communicating the importance of effective information security management and ensuring that the information security management system achieves its intended outcome(s).

5.1.8 To identify all assets that directly or indirectly impact the operations, and understand their vulnerabilities and the threats through appropriate risk assessment

5.1.9 To comply with applicable laws and contractual obligations pertaining to information security and data privacy, for its internal data and intellectual property related data.

5.1.10 Directing and supporting persons to contribute to the effectiveness of the information security management system.

5.1.11 Promoting continual improvement of ISMS.

5.1.12 To raise awareness of information security risks within Morepen Laboratories Limited and create and maintain a security-conscious culture ensuring that all breaches of information security and suspected weakness are reported, investigated and adequate actions are taken.

# 6. Policies for Information Security

## *6.1. Review of Information Security Policy.*

6.1.1. The policy shall be reviewed at least once in a year and at a time of any major change(s) in the existing environment affecting the policies and procedures. Information Security Policy shall be reviewed by the IT Head and approved by Senior Management. The reviews shall be carried out for assessing the following: -

6.1.1.1. Impact on the risk profile due to, but not limited to, the changes in information assets, deployed technology/ architecture, regulatory and/ or legal requirements, emerging threat landscape;

6.1.1.2. Effectiveness of the policies;

6.1.1.3. Feedback based on the business needs and requirements;

6.1.1.4. Change in the business;

6.1.1.5. Change in the IT environment;

6.1.1.6. Trends related to threat and vulnerabilities; and

6.1.1.7. Reported security incidents and audit findings.

The Information Security policy should be read in conjunction with Morepen Laboratories Limited's supporting policies and procedures as follows:

- Acceptable Usage Policy
- Access Control Policy
- Access Control Procedure
- Asset Management Policy
- Asset Management Procedure
- Business Continuity Plan
- Business Continuity Policy
- Change Management Policy
- Change Management Procedure
- Communication Security Procedure
- Cryptography and key management Policy
- Human Resource Security Policy
- Human Resource Security Procedure
- Incident Management Procedure
- Information Security Policy
- Internal Audit Procedure

- Operational Security Management Policy
- Operations Security Procedure
- Physical and Environmental Security Policy
- System Acquisition Development and Maintenance Policy
- Training and Awareness Policy

Latest & approved copies of Information Security policies & supporting documents available on **INTRANET**.

## 6.2. Organization of Information Security

6.2.1. Morepen Laboratories Limited shall define appropriate role, responsibilities and authority to manage information security across all functions. Relevant stakeholders and experts shall be identified from various departments, divisions and locations to ensure structured co-ordination of information security related activities.

## *6.3. Human Resource Security*

6.3.1. Morepen Laboratories Limited should formulate Human Resource Policy aiming to ensure that all workforce members working for Morepen Laboratories Limited are suitable for the roles they are hired for and are made aware of their responsibilities for ensuring availability and protecting, confidentiality & integrity of Morepen Laboratories Limited information assets and customer information to which they have access. It specifies the information security requirements that shall be integrated in the HR processes during recruitment, employment and separation.

6.3.2. Appropriate controls shall be established to ensure that employees and third parties contractors, consultants, vendors, trainees etc. understand their responsibilities and suitable controls are implemented for reducing risk of theft, fraud and misuse of information.

## *6.4. Asset Management*

6.4.1 Morepen Laboratories Limited shall document and maintain a Asset Management policy and procedure to achieve and maintain appropriate protection of Morepen Laboratories Limited information assets against all information security risks.

### 6.4.2 Responsibility for Asset

6.4.2.1 All the information assets shall be protected based on their Confidentiality, Integrity and Availability (CIA) requirements.

### 6.4.3 Information Classification

6.4.3.1The criteria for identification, ownership, valuation, classification and handling of the information assets shall be established.

### 6.4.4 Labelling of Information

6.4.4.1An appropriate set of procedures for information labeling shall be developed and implemented in accordance with the information classification scheme adopted by the , Asset tags may be used to group IT assets under a specific classification.

6.4.4.2Morepen Laboratories Limited Shall ensure that Asset owners shall label their assets. The following assets shall have label/asset tag

6.4.4.2.1 Endpoints including mobile devices

6.4.4.2.2 Servers

6.4.4.2.3 Network devices

6.4.4.2.4 Systems & Applications

6.4.4.2.4 Physical assets

6.4.4.3Morepen Laboratories Limited shall ensure that people under its control are made aware of the definition of Personal Identified Information(PII) and how to recognize information that is PII.

### 6.4.5 Handling of Assets

6.4.5.1The asset inventory shall be reviewed by asset owners on an annual basis or business requirements whenever there is any change in the inventory.

6.4.5.2Copies, both temporary and permanent, of the information asset, shall be protected and stored to a level consistent with the protection of the original information

### 6.4.6 Media Handling

6.4.6.1To prevent unauthorized disclosure, modification, removal or destruction of information stored on removable media.

## *6.5. Access Control*

6.5.1 Morepen Laboratories Limited shall formulate a Access control policy and procedure to implement Access Control across all IT systems and services in order to provide authorized, and appropriate user access and to ensure appropriate preservation of data Confidentiality, Integrity and Availability

6.5.2 Organization shall ensure that access to the Morepen Laboratories Limited's information systems is granted only after authorized approval on the basis of need-to-know principle

### 6.5.3 Business Requirement of Access Control

6.5.3.1 Appropriate logical access controls shall be established to safeguard the Information Assets. Access be given in case of business needs shall be Role-Based Access Control (RBAC) and for a fixed period of time.

### 6.5.4 User Access Management

6.5.4.1 Conduct automated/manual and regular access reviews of privileged user as well as non-privileged users.

6.5.4.2 Immediately deactivate and promptly delete user IDs after an employee leaves.

6.5.4.3 Implement strict monitoring and control mechanisms for third-party access.

### 6.5.5 User Responsibilities

6.5.5.1 All employees with access to information assets are required to understand their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

### 6.5.6 System and Application Access Control

6.5.6.1 Adequate measures shall be undertaken to prevent un-authorized access to the systems and applications used within Morepen Laboratories Limited 's IT facilities.

## *6.6. Physical and Environmental Security*

6.6.1. Physical and environmental security shall be implemented to prevent unauthorized physical access, damage, and interference to the Morepen Laboratories Limited 's premises.

### 6.6.2. Secure Areas

6.6.2.1. To ensure that access to secure areas is restricted and is on need basis only.

### 6.6.3. Equipment

6.6.3.1. Appropriate measures shall be adopted to ensure that all equipment are located, maintained and protected against loss and damage.

## *6.7. Operation Security*

6.7.1 Morepen Laboratories Limited shall document and maintain a Operational security policy and procedure to ensure the correct and secure operation of information processing facilities.

### 6.7.2 Operational Procedure and Responsibilities

6.7.2.1 To ensure that operating procedures are correct, updated and accessible when needed.

### 6.7.3 Protection from Malwares

6.7.3.1 Appropriate measures shall be taken to protect Morepen Laboratories Limited 's information systems from the damage caused by malicious and mobile code.

### 6.7.4 Backup

6.7.4.1 Adequate backup and recovery procedures shall be in place to ensure that business critical software, data and documentation is recoverable in a timely manner in the event of corruption or failure of Morepen Laboratories Limited 's information systems

### 6.7.5 Logging and Monitoring

6.7.5.1 Adequate measures shall be defined and implemented to monitor information systems to record and maintain events created whenever user logs on to information systems.

### 6.7.6 Technical Vulnerability Management

6.7.6.1 Morepen Laboratories Limited 's information systems shall be periodically checked (at least once every year) to confirm compliance with its security implementation standards.

6.7.6.2 Establish a consistent and regular schedule for deploying patches to ensure timely updates and minimize vulnerabilities. This schedule should include routine patches as well as an expedited process for critical or emergency patches

6.7.6.3 Implement a process for testing patches in a controlled environment before deployment to production systems. This ensures that patches do not negatively impact system performance or compatibility, reducing the risk of operational disruptions.

6.7.6.4 Key Performance Indicators (KPIs) shall be maintained and reported to senior management with respect to technical vulnerability management.

### 6.7.7 Information System Audit Considerations

6.7.7.1 Adequate measures shall be taken to maximize the effectiveness and to minimize the interference to/ from information systems audit process.

## *6.8 Communication Security*

6.8.1 Communication security shall be ensured by the protection of information in networks and its supporting information processing facilities and maintain the security of information transferred within Morepen Laboratories Limited and with any external entity.

6.8.2 MOREPEN LABORATORIES LIMITED shall assess the necessity of internal and external communications pertaining to the information security management system, including:

6.8.2.1 Determining the content of communication.

6.8.2.2 Establishing the timing of communication.

6.8.2.3 Identifying the recipients of communication.

6.8.2.4 Designating responsible parties for communication.

6.8.2.5 Specifying the processes for conducting communication.

### 6.8.3 Network Security Management

6.8.3.1 Security of network assets managed by Morepen Laboratories Limited is of significant importance and the communication network shall be protected appropriately against the threats to the network.

### 6.8.4 Information Transfer

6.8.4.1 To maintain the security of information transferred within Morepen Laboratories Limited and with any external entity. Information exchange within Company and to external parties needs to be controlled to prevent loss, modification and misuse of information.

## *6.9 System Acquisition, Development and Maintenance*

6.9.1 System Acquisition, Development and Maintenance Policy shall be developed to ensure that information security is integral part of information system development and maintenance.

### 6.9.2 Security Requirements of Information System

6.9.2.1 To ensure that information security as an integral part of information technology systems across the entire lifecycle including the requirements for information technology systems which provide services over public networks the organization shall document controls to fulfill this requirement.

### 6.9.3 Security in Development and Support Processes

6.9.3.1 Morepen Laboratories Limited to ensure that information security is designed and implemented within each phase of development of information systems lifecycle.

### 6.9.4 Test Data

6.9.4.1 Avoid using any real or production data for testing purpose.

6.9.4.2 Ensure that sensitive data is anonymized or masked before being used in testing environments. This helps protect personally identifiable information (PII) and other sensitive data from unauthorized access and reduces the risk of data breaches.

6.9.4.3 Implement processes to ensure the integrity and accuracy of test data. This includes validating test data to ensure it accurately reflects the conditions and scenarios being tested, and regularly auditing test data to detect and correct any discrepancies or errors.

## *6.10 Supplier Relationship*

6.10.1 Morepen Laboratories Limited to ensure protection of the organization's assets that is accessible by suppliers and implement relevant security controls to monitor and evaluate supplier relationship

### 6.10.2 Information Security in Supplier Relationships

6.10.2.1 Conduct thorough security assessments and due diligence on all potential suppliers before engaging in a relationship. This includes evaluating the supplier's

security practices, policies, and history of data breaches or security incidents. Regularly review and reassess the security posture of existing suppliers.

6.10.2.2 Include specific security requirements and clauses in contracts with suppliers. These should cover aspects such as data protection, confidentiality, breach notification, and compliance with relevant regulations and standards. Ensure that suppliers are contractually obligated to adhere to the organization's security policies and procedures.

6.10.2.3 Implement a process for ongoing monitoring and auditing of suppliers' security practices. This includes regular audits, security reviews, and continuous monitoring of suppliers' compliance with security requirements.

#### 6.10.3 Supplier Service Delivery Management

6.10.3.1 Establish clear performance metrics and service level agreements (SLAs) to monitor and evaluate supplier performance. Regularly review and assess supplier performance against these metrics to ensure they meet the agreed-upon standards and address any issues promptly.

6.10.3.2 Implement a risk management framework to identify, assess, and mitigate risks associated with supplier service delivery. Develop and maintain contingency plans to address potential disruptions, ensuring continuity of operations in case of supplier failure or other issues affecting service delivery.

## *6.11 Information Security Incident Management*

6.11.1 Morepen Laboratories Limited to ensure that Incident Management procedure is developed and maintained to defines the process for managing security incidents and weaknesses.

6.11.2 Ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

6.11.3 Incident management roles & responsibilities shall be identified, assigned and reviewed on periodic basis.

## *6.12 Information Security Aspects of Business Continuity Management*

6.12.1 Morepen Laboratories Limited shall formulate Business Continuity policy and procedure to minimize interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters ensure their timely resumption.

6.12.2 Periodic and adequate tests/ drills shall be performed as per business continuity plans

#### 6.12.3 Supplier Service Delivery Management

6.12.3.1 Information security continuity shall be identified and adhered to during the time of a disaster.

## *6.13 Compliance*

**6.13.1** Morepen Laboratories Limited to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements as defined by organization's policy, procedure, compliance standard or regulatory guidelines.

## *6.14 Risk Management Policy*

6.14.1When planning for the information security management system, the organization shall consider the internal and external issues and the Legal and regulatory requirements and contractual obligations and determine the risks and opportunities that need to be addressed to:

6.14.1.1 Ensure the information security management system can achieve its intended outcome.
6.14.1.2 Prevent, or reduce, undesired effects and achieve continual improvement.
6.14.1.3 The organization shall plan actions to address these risks and opportunities and how to integrate and implement the actions into its information security management system processes and evaluate the effectiveness of these actions.

### 6.14.2 Risk Assessment

6.14.2.1 Morepen Laboratories Limited shall perform information security risk assessments at planned intervals.

6.14.2.2 Morepen Laboratories Limited shall implement an information security risk assessment process that:

6.14.2.3 Defines and maintains information security risk criteria, including:

6.14.2.3.1 Criteria for accepting risks.

6.14.2.3.2 Criteria for conducting information security risk assessments.

6.14.2.4 Ensures consistency, validity, and comparability in the results of repeated information security risk assessments.

6.14.2.5 Identifies information security risks.

6.14.2.5.1 Applies the information security risk assessment process to identify risks related to the loss of confidentiality, integrity, and availability of information within the scope of the information security management system.

6.14.2.5.2 Identifies the owners of those risks.

6.14.2.6 Analyzes information security risks.

6.14.2.6.1 Assesses the potential consequences if the identified risks were to materialize.

6.14.2.6.2 Assesses the realistic likelihood of the identified risks occurring and determines their risk levels.

6.14.2.7 Evaluates information security risks.

6.14.2.7.1 Compares the results of risk analysis with established risk criteria and prioritizes analyzed risks for risk treatment.

**6.14.3** Documented information about the information security risk assessment process must be maintained by the organization.

6.14.3.1 The organization is mandated to establish and enact an information security risk treatment process to:

6.14.3.1.1 Select suitable information security risk treatment options, taking into account the outcomes of the risk assessment.

6.14.3.1.2 Identify all necessary controls needed to implement the chosen information security risk treatment options.

6.14.3.1.3 Compare the controls outlined in 6.14.3.1.2 with those detailed in Annex A to ensure no essential controls have been overlooked.

6.14.3.1.4 Formulate a Statement of Applicability containing the required controls along with justifications for their inclusion or exclusion from Annex A, whether implemented or not.

6.14.3.1.5 Develop an information security risk treatment plan.

6.14.3.1.6 Secure approval from risk owners for the information security risk treatment plan and acceptance of residual information security risks.

6.14.3.2 The organization is required to retain documented information regarding the information security risk treatment process.

## *6.15 Competency*

6.15.1 Morepen Laboratories Limited shall determine the essential expertise of individuals carrying out tasks under its authority that impacts its information security performance.

6.15.2 Ensure that these individuals possess the requisite competence through appropriate education, training, or experience.

6.15.3 Implement necessary measures, as applicable, to attain the required competence and assess the efficacy of such measures.

6.15.4 Retain pertinent documented evidence as proof of competence.

## *6.16 Data Privacy*

6.16.1 Data privacy describes a set of principles and guidelines to ensure the respectful processing, protection, and handling of sensitive data linked to a person. This concept ties to who can define, observe, use, and control a person's information and how.

6.16.2 Organization should employ security measures, including encryption, secure access controls, and regular security audits, to safeguard personal information against unauthorized access, disclosure, or destruction

6.16.3 Organization shall collect only the data necessary for specific purposes and avoid excessive data collection. Regularly review and delete data that is no longer needed.

## 7. Policy Awareness and Training

7.1 Morepen Laboratories Limited shall periodically communicate the importance of maintaining information security by employing means such as mailers, posters etc. to all its personnel including suppliers and third parties and the consequences of not complying with the requirements of the information security management system.

7.2 Periodic training shall also be provided regarding maintaining information security from time to time. Records of which shall be maintained for desired amount of time.

7.3 Human link is the weakest link in the information security chain. Hence, there is a vital need for an initial and ongoing training and information security awareness program. The program may be periodically updated keeping in view changes in information technology system, threats/vulnerabilities and/or the information security framework.

7.4 Organization shall implement a mechanism to track the effectiveness of training programs through an assessment / testing process including the benefits of improved information security performance. At any point of time, Morepen Laboratories Limited may needs to maintain an updated status on user training and awareness relating to information security.

## 8. Documented Information

8.1 The organization's information security management system shall encompass:

8.1.1 Documented information needed for setting up the information security management system.

8.1.2 Documented information identified by the organization as essential for the effectiveness of the information security management system.

### 8.2 Control of Documents and Records:

8.2.1 When creating and updating documented information, the organization shall ensure:

8.2.1.1 Proper identification and description, such as a title, date, author, or reference number.

8.2.1.2 Suitable format, including language, software version, and graphics, as well as appropriate media, such as paper or electronic.

8.2.1.3 Review and approval for suitability and adequacy.

8.2.2 The documented information required by the information security management system shall be managed to ensure:

8.2.2.1 Availability and suitability for use, whenever and wherever needed; and

8.2.2.2 Adequate protection against risks such as loss of confidentiality, improper use, or loss of integrity.

8.2.2.3 For the management of documented information, the organization must undertake the following activities, as applicable:

8.2.2.4 Distribution, access, retrieval, and use.

8.2.2.5 Storage and preservation, including the maintenance of legibility.

8.2.2.6 Control of changes, including version control.

8.2.2.7 Retention and disposal.

8.2.2.8 Documented information of external origin, deemed necessary by the organization

for the planning and operation of the information security management system, must be appropriately identified and managed.

# 9 Performance Evaluation

## 9.1 Monitoring, measurement, analysis and evaluation

9.1.1 The organization must assess the performance of information security and the effectiveness of the information security management system.

9.1.2 The organization should determine:

9.1.2.1 What needs to be monitored and measured, including information security processes and controls.

9.1.2.2 The methods for monitoring, measurement, analysis, and evaluation, as applicable, to ensure valid results.

9.1.2.3 When monitoring and measurement should take place.

9.1.2.4 Who should be responsible for monitoring and measurement;

9.1.2.5 When the results from monitoring and measurement should be analyzed and evaluated.

9.1.2.6 Who should analyze and evaluate these results.

9.1.2.7 The organization must maintain appropriate documented information as evidence of the monitoring and measurement results.

## 9.2 Internal Audit

9.2.1 The organization shall conduct internal audits at planned intervals in accordance with Internal audit procedure to determine whether the information security management system:

9.2.1.1 Conforms to the organization's own requirements for its information security management system and is effectively implemented and maintained.

9.2.1.2 The organization shall Plan, establish, implement, and maintain audit programs, including defining the frequency, methods, responsibilities, planning requirements, and reporting. The audit programs shall consider the importance of the processes involved and the findings of previous audits.

9.2.1.3 Define the audit criteria and scope for each audit.

9.2.1.4 Select auditors and conduct audits to ensure objectivity and impartiality in the audit process.

9.2.1.5 Ensure that audit results are reported to relevant management; and

9.2.1.6 Retain documented information as evidence of the audit program(s) and audit results.

## *10 Exceptions and Non-Compliance*

10.1 All exceptions from this policy should be approved from the IT Head/Senior Management and be documented with justification. Any unapproved deviation i.e. non-compliances from the policy shall be dealt with action as defined appropriate by the legal and HR function in consultation with the IT Head and Senior Management.

10.2 A tracker of all the exceptions to the policy shall be maintained and reviewed by the Morepen Laboratories Limited.

## *11 Enforcement*

11.1 All employees are expected to comply with the Morepen Laboratories Limited's Information Security Policy. Non-compliance with the same shall result in disciplinary action or punishment, which shall vary as per the severity of the incidence.