SUN PHARMACEUTICAL INDUSTRIES LIMITED

Information Security Policy (ISP)

Version: 1.0

Document No: ISMS-PL_00001

Table of Contents

Signatures

By signing below, the individuals listed have reviewed and approved this document.

Author			
Name	**Designation**	**Signature**	**Date (DD-MMM-YY)**
Mahesh Sukale	Sr. Manager	Mahesh Sukale	Digitally signed by Mahesh Sukale DN: c=IN, st=Maharashtra, l=Mumbai, 2.5.4.97=VATIN-27AADCS3124K1ZD, cn=Sukale, givenName=Mahesh, o=SUN PHARMACEUTICAL INDUSTRIES LIMITED, cn=Mahesh Sukale, email=mahesh.sukale@sunpharma.com Date: 2026.02.18 19:47:50 +05'30'

Reviewed/Owned By			
Name	**Designation**	**Signature**	**Date (DD-MMM-YY)**
Usman Kathi	Global CISO	Usman Kathi	Digitally signed by Usman Kathi DN: c=IN, st=Maharashtra, l=Mumbai, 2.5.4.97=VATIN-27AADCS3124K1ZD, cn=Kathi, givenName=Usman, o=SUN PHARMACEUTICAL INDUSTRIES LIMITED, cn=Usman Kathi, email=Usman.Kathi@sunpharma.com Reason: I have reviewed this document Location: Mumbai Date: 2026.02.23 15:50:28 +05'30'

Approved By			
Name	**Designation**	**Signature**	**Date (DD-MMM-YY)**
Dheeraj Sinha	Group CIO		Dheeraj Sinha 2026.02.26 12:13:08 +05'30'

Version	**Revision Date** (DD-MMM-YY)	**Summary of changes**	**Updated By**
1.0	N.A.	Initial Document	N.A.

1. Purpose

The purpose of the Information Security Policy Document is to communicate Sun Pharmaceutical Industries Limited's (hereinafter referred to as SPIL) information security framework to partners and stakeholders. This document outlines the key policy coverage areas implemented by SPIL.

2. Objective

The objective of this Information Security Policy is to:

- **Protect Information Assets and Infrastructure**
  To safeguard SPIL's information assets and supporting infrastructure, including those owned by SPIL as well as by business partners involved in SPIL operations.

- **Demonstrate Commitment to Information Security:**
  The implementation of this policy reflects SPIL's ongoing commitment to maintaining and enhancing its information security initiatives, thereby instilling confidence in stakeholders and customers regarding the security of its business practices.

- **Ensure the CIA Triad**
  To protect the confidentiality, maintain the integrity, and ensure the availability of information and information systems.

- **Establish Roles and Responsibilities**
  To define and communicate responsibilities for information security across the entire workforce, ensuring accountability at all levels.

- **Define Security Requirements for Third Parties**
  To establish clear information security requirements for third parties, including vendors, service providers, and business partners from IT, HR, Admin and Security, Legal and other associated departments.

- **Manage Information Security Risks**
  To identify, assess, and manage information security risks to an acceptable level through the design and implementation of a comprehensive risk management framework.

- **Incident Response and Recovery**
  To respond to and recover from information security incidents effectively and in a timely manner.

- **Promote Security Awareness**
  To foster a culture of information security awareness among employees, service providers, and customers.

- **Legal and Regulatory Compliance**
  To comply with applicable legal, regulatory, and contractual requirements related to information security.

- **Continuous Improvement of Information Security Systems**
  To continuously monitor, review, and improve information security systems, processes, and controls in alignment with evolving threats, technologies, and business needs.

3. Scope

This policy applies to Sun Pharmaceutical Industries Limited, its subsidiaries and affiliates (hereinafter referred to as 'Sun Pharma' or 'SPIL'). It outlines the rules and guidelines for safeguarding all information assets, systems, and technologies owned, operated, or managed by the Sun Pharma. This policy applies to all employees, vendors, contractors, third-party service providers, and any other individuals involved in managing relevant IT processes and information within Sun Pharma, subsidiaries and affiliates.

Note - This policy will / may not directly apply to all GXP systems, as separate GSOPs are documented, applicable and implemented for them. The existing GSOP will precede this policy.

4. Responsibility

It is the responsibility of Group CIO / Group CISO with help of Information Security team to ensure that the Information Security Policies as mentioned below are complied with by all relevant stakeholders.

5. Policy Compliance and review

This policy shall be reviewed at least annually or on any major change to ensure its continued suitability and effectiveness. This policy shall comply with the regulations, laws, and frameworks applicable to SPIL.

6. Information Security Policy Statements

6.1 Policy for Information Security

This policy highlights the senior management's intention to identify and secure organization's valuable assets, in a manner which complies with legislations, meets leading practices and business needs, protecting it from unauthorized use, disclosure, or destruction.

6.2 Organization of Information Security

- The organization shall establish a clear and effective framework for managing information security by defining roles, responsibilities, and reporting lines to ensure accountability and oversight. A designated Information Security Officer or team will be responsible for developing, implementing, and maintaining security policies and procedures.
- Departments and personnel must collaborate to uphold information security objectives, with specific security responsibilities assigned according to job functions. Coordination with external parties will be managed to maintain security standards, and regular communication and training will support a strong security culture throughout the organization. This structure will be reviewed periodically to ensure it remains effective and aligned with the organization's goals.

6.3 Acceptable Usage

- Acceptable use of information processing resources is defined in 'Acceptable Usage Policy' and acknowledged by users.

- The Acceptable Usage Policy covers following areas as part of acceptable usage:
  - Handling of Information as per their classification.
  - Acceptable use of IT and Information assets.
  - Safe Usage of Internet Access.
  - Safe usage regarding Password and Secret authentications codes.
  - Social Media Usage.
  - Awareness about Phishing, Vishing, Quishing, Smishing attacks.
  - Secure practices for Email and Communication channel use.
  - Clear Desk and Clear Screen Practices.
  - Security of assets while out of office and during travel and official stays.
  - Handling of customer information.
  - Privacy Data related awareness.
  - Use of Artificial Intelligence.
  - Employees and vendors shall be responsible for proper use and safeguarding of SPIL's information resources.

6.4 Human resource security

- SPIL has created Human Resource Security Policy that covers following aspects of Human Resource Security in Human Resource processes:
  - Screening and Background Verification Employment terms shall include responsibilities for information security, Security awareness training during induction and regular update on the awareness.
  - Disciplinary processes to address security incidents.
  - Non-disclosure agreements during employment and post-employment.
  - Return of assets during exit or separation from the group.
  - Change and / or Removal of accesses while role change or changing to other SPIL Group entity or exit from the Group.
  - Security practices when employee is allowed remote working.
  - Awareness about security event or security incident reporting.

6.5 Asset management

- SPIL has an Asset Management Policy to cover following area of Asset management:
  - Identify Information Assets with their owners and maintain an inventory.
  - Inclusion of Software Assets, Physical Assets and necessary license management.
  - Provision of asset allocation, movement and return.
  - Security controls while onboarding assets like baselining.
  - Replacement / Disposal of asset when its life is complete or its purpose is over.
  - Considering removal of information, licenses before disposal.
  - Secure disposal considering E-Waste management rules.

6.6 Identity and access management

- SPIL has an Identity and Access Management Policy which covers following aspects of Identity and Access Management:
  - User registration and de-registration process for assigning access rights.

- Assign unique user IDs and passwords with a formal process for creation, modification, and deletion.
- Authorization from the Business and Department head for user access requests.
- Allocating privileges access to any user id.
- Management of Administrative and Privilege accesses.
- Review of Accesses including Administrative and Privilege accesses.
- Removal or disabling unused ID and / or accesses.

6.7 Password security

- SPIL has Password Management Policy to manage secret authentication information (e.g., passwords, encryption keys) for all logins and privileged accounts.
- Passwords must meet complexity requirements, and SPIL users shall keep them confidential.
- Any access provided to privileged users and users outside the SPIL environment e.g., Remote access shall have Multi-Factor Authentication (MFA) in place.

6.8 Information security risk assessment and management

- SPIL has an Information security risk assessment and management policy and every IT system or process supporting business functions at SPIL shall undergo information risk management and receive information risk assessments, conducted at least annually.
- Information security risk assessments are required for new IT projects, the implementation of new technologies, significant alterations to the operating environment, or when a significant vulnerability identified.
- The Risk Management process covers Risk Assessment, Risk Analysis, Risk Evaluation, Risk Mitigation and Residual Risk Acceptance.

6.9 Information classification and handling

- Based on the criteria defined in Information security risk assessment and management policy Information Assets and processing systems shall be classified by legal requirements, sensitivity, and criticality to business.
- Policy covers the Security of information during transmission, communication, processing from its creation to its disposal / destruction based on its category.
- Information Assets shall be classified as per established standard in the following categories:
  - Confidential
  - Restricted
  - Internal
  - Public

6.10 Change Management

- SPIL has Change management policy to comprehensively cover clear documentation of the scope, classification, validation, approval, and prioritization of changes, including a detailed analysis of business benefits, risks, impact, and rollback plans.
- The policy also covers Testing of Changes, Change Approval Boards, Security assessment of changes, treatment of Test Data, availability of UAT / Test environment for changes, Segregation of test and development facilities, access provisioning of developer and tester into various environments.

6.11 Backup and Restoration Management

- SPIL has Backup and Restoration policy to ensure the availability of critical business information, software, and device configurations during emergencies.
- The policy covered provision of identifying backup requirements, backup frequency and schedule, Backup media management including labelling and offsite media rotation, Backup testing and Restoration testing, Backup Retention, Archival.
- Backup failures are to be treated as IT incidents and Root Cause Analysis for failures and adequate controls will apply.

6.12 Capacity Management

- SPIL has Capacity Management policy to identify critical IT resources, including business-critical applications, operating systems, databases, hardware, networking components, data files, and network connectivity.
- The policy provision includes monitoring of critical parameters and their thresholds, Capacity trends including new business requirements with an objective that results of capacity planning may be included in future capacity augmentation, planning and improvement.

6.13 Logging and Monitoring

- SPIL has Logging and Monitoring policy to ensure that user activities, exceptions, and security events shall be logged and monitored.
- The policy includes provision of logging and monitoring, log reviews, log retentions as per business and regulatory requirements, protections of logs form destruction and unauthorised access.
- SPIL gathers threat intelligence feeds or alerts from various external sources such as Vendor (OEM) Reports, Government Agencies (CERT-IN), Subscription to publicly available Threat Intel web sources and analyses the feeds as per the existing threat vector or landscape and take appropriate action in enhancing the defence mechanisms like monitoring and malware controls.
- SPIL implemented brand monitoring mechanisms to detect and respond to any misuse of the SPIL's brand, trademarks, or identity across digital platforms, social media, and external sources to prevent reputational damage and fraudulent activities.

6.14 Cryptography

- SPIL has a Cryptography Policy to ensure that encryption levels align with information criticality, information security requirements employing standard and updated technology unless a deviation mandated by regulations.

6.15 Physical and environmental security

- SPIL has a Physical and Environmental Security Policy to:
  - Implement entry level security measures like fencing, entry control, and manned reception desks, visitor management systems, physical access controls, gate passes etc. for protection.
  - The policy includes provisions of securing facility perimeter, equip public zone doors with locks, CCTV surveillance, Zoning, secure storage, fire protection, Clear desk and space, secure and safe equipment siting, and deploy round-the-clock security.

6.16 Network Security Management

- SPIL has Network Security Management Policy to secure and protect communication channels and devices including network components, links, end user systems, LAN and WAN provisioning, Network Zoning, Email Security etc.
- The policy also covers the provisions of secure sharing of information, Remote Working controls, VPN usage.

6.17 Secure Software development lifecycle management

- SPIL has a Secure Software development lifecycle management Policy to manage the Software Acquisition, Development, Change and Maintenance.
- The policy includes provisioning secure environment for software and system development by using secure coding practices, define acceptance criteria and rollout after security testing. Restrict and monitor access to the development environment.

6.18 Third party security

- SPIL has a Third-Party Security Policy to manage the outsourcing of IT / IS systems and services.
- The policy provisions include security consideration in third party selection, defining their criticality, having NDA and SLA, measuring performance, manging third party personnel and their accesses, performing regular risk assessments, managing changes in third parties and handovers.

6.19 Information security incident management

- SPIL has Information Security Incident Management Policy is to ensure a timely and effective response to security incidents.
- The policy provisions include proving channel of reporting events and incidents, their acknowledgement, taking immediate action to contain the impact, Root Cause Analysis, Corrective action planning, capturing learning from the incidents for training and future planning purpose and keeping records for incident purpose, with provision of reporting to any regulatory or statutory bodies and impacted customers and personnel.
- SPIL has opted for cyber insurance to compensate in case of any loss because of cyber or information security incidents.

6.20 Information Security in Business continuity Arrangements

- SPIL has Information Security Continuity Policy to ensure that it shall maintain ICT security in line with Confidentiality, Integrity, and Availability principles during business continuity situations.
- The provision of the policy includes, including SPIL continuity requirements in supplier agreements, conduct periodic test of Information Security Continuity, and regularly update Information Security Continuity arrangements.

6.21 Sustenance and Compliance management

- SPIL has Information Security Sustenance and Compliance Policy to ensure continued compliance with SPIL's information security policies and procedures, and other regulatory and customer requirements.
- The provision includes to carryout audits and assessments, issue identification, closures and reporting at relevant levels.

6.22 Mobile device Management

- SPIL has Mobile Device Management Policy to address security on mobile devices accessing SPIL' network including smartphones, or other smart mobile devices. These must be secured with strong passwords and encryption.
- The provisions of the policy include having a central control for mobile devices to ensure security on all devices, enforce secure remote work practices, securing company data on mobile devices and wiping if necessary.

6.23 Cloud security

- SPIL has a Cloud Security Policy to manage the usage and security of cloud resources services with respect to due diligence in selection of partners and applying technical controls.
- The policy includes the provisions like localisation of sensitive data, if required, cloud access monitoring, technical vulnerability testing etc.

6.24 Data privacy, protection and lifecycle management

- SPIL has published its privacy policy on website.
- SPIL has included provision of data privacy in its Information Security Sustenance and Compliance Policy and Procedure to ensure privacy and protection of personally identifiable information per relevant laws.

6.25 Malware Protection

- SPIL has Malware Protection Policy to Implement anti-malware mechanisms to detect, prevent, and recover from malware, Keeping Endpoint detection and response (EDR) installed and up to date and Scan and quarantine emails, attachments, downloads, removable media for malicious code and disable auto-run on all media.

6.26 Information Security Audit

- SPIL has Information Security Audit Policy to timely inform on ISMS gaps, vulnerabilities through VAPT or from other trusted sources, third-party audit and act upon them to close the reported weaknesses.

6.27 Configuration management

- SPIL has included configuration in Asset Management to defined configurations for all systems (Servers, Endpoints, Network Devices, Operating Systems, Databases, Application and Services etc) including cloud services, with roles and responsibilities for enforcement, and update on configurations.

7. Exceptions

Exceptions if any, to be managed as per the defined exception management procedure with valid business justification and approvals.

8. Violations

Failure to comply with the Information Security Policy can result in disciplinary action, up to and including termination and legal action. Violations of this policy should be reported to the SPIL's Information Security Office at isecure@sunpharma.com

9. Documentation

The Information Security Team shall be responsible for the overall documentation required to ensure adherence to this policy and deviations to this policy by any user shall be recorded by the team.