Information Security Policy

DOCUMENT CLASSIFICAION:	Internal Use
DOCUMENT NO:	IT – 001 / 02
REVISION NO:	02
DATE OF REVISION:	15/07/2026
PREPARED BY:	Sahil Shaikh (AM Infosec)
SIGNATURE:	
REVIEWED BY:	Nirav Desai (AGM IT)
SIGNATURE:	
APPROVED BY:	Sudhesh Mishra (COO)
SIGNATURE:	

Revision

REV NO	REV DATE	SECTION	SUMMARY OF CHANGES	PREPARED BY	AUTHORIZED BY
02	15/07/26	1, 6, 7, 8, 10	Revision of Information Security Policy: regulatory references expanded (GxP, EMA, CDSCO) in Sec. 1; Data Privacy Function, Procurement Team, HR Team and Suppliers & Third Parties added to Sec. 6; supplier non-compliance consequences and external incident escalation added to Sec. 7; review triggers and ISMS review inputs expanded in Sec. 8; new Sec. 10 Information Security Targets and KPIs added. Ref: CHG-2026-002.	Sahil Shaikh (AM Infosec)	Nirav Desai(AGM IT)

Distribution

DISTRIBUTED TO	POSITION	DATE	SIGNATURE

Approval

NAME	POSITION	DATE	SIGNATURE
Nirav Desai	AGM IT	15/07/2026	

INFORMATION SECURITY POLICY

1. Introduction

This Information Security Policy defines the overall information security objectives, principles, and governance framework of Farmson Basic Drugs Private Limited.

Farmson Basic Drugs Private Limited recognizes that information is a critical business asset and must be protected against unauthorized access, disclosure, alteration, loss, or destruction. Senior management is fully committed to ensuring that information security supports uninterrupted business operations, regulatory compliance, and stakeholder trust.

The organization has implemented an Information Security Management System (ISMS) in alignment with **ISO/IEC 27001:2022** and applicable pharmaceutical and regulatory requirements, including but not limited to **GxP guidelines, FDA 21 CFR Part 11, EMA, CDSCO**, and the **Digital Personal Data Protection (DPDP) Act, 2023**.

2. Objectives of Information Security

The objectives of this policy are to:

- Protect confidentiality, integrity, and availability of information assets
- Ensure compliance with legal, regulatory, contractual, and statutory requirements
- Maintain business continuity and system availability
- Protect intellectual property, formulations, and proprietary information
- Prevent data breaches, cyberattacks, and data manipulation
- Foster a culture of information security awareness and continual improvement

3. Scope and Applicability

This policy applies to:

- All employees, directors, board members, interns, contractors, suppliers, and third parties who interact with company IT assets.
- All information assets, systems, applications, networks, and processes
- Information processed in electronic, physical, or verbal form

Compliance with this policy is mandatory for all individuals and entities within scope.

4. Information Security Governance

Farmson Basic Drugs Private Limited has established an Information Security Management System (ISMS) to systematically manage information security risks.

4.1 Information Security Requirements

- Business, legal, regulatory, and contractual information security requirements shall be identified, documented, and maintained.
- Security requirements for new or changed systems shall be defined during design and implementation stages.
- Information security controls should be driven by business needs and risk assessments.

4.2 Continual Improvement of ISMS

The organization is committed to continual improvement of the ISMS through:

- Regular risk assessments
- Internal audits and management reviews
- Monitoring security metrics and performance indicators
- Corrective and preventive actions
- Feedback from employees and regulators

5. Information Security Policy Framework

This Information Security Policy is supported by a comprehensive set of domain-specific policies that define detailed controls and responsibilities.

These policies are approved by management, communicated to relevant stakeholders, and reviewed periodically.

5.1 Supporting Information Security Policies

The ISMS policy framework includes, but is not limited to, the following policies

- Information Security Policy
- Internet Access Policy
- Web Filtering Policy
- Cloud Services Policy
- Access Control Policy
- Anti-Malware Policy
- CCTV Surveillance Policy
- Data Backup Policy
- Logging & Monitoring Policy

- Software Policy
- Network Security Policy
- Electronic Messaging Policy
- Availability Management Policy
- Asset Management Policy
- HR Security Policy
- Physical Security Policy
- Clear Desk & Clear Screen Policy
- Acceptable Use Policy
- Remote Work Policy
- Information Transfer Policy
- Incident Response Policy
- Threat Intelligence Policy
- Data Leakage Prevention (DLP) Policy
- Patch Management Policy
- Vulnerability Management Policy
- Data Retention & Disposal Policy
- Vendor & Third-Party Security Policy
- Change Management Policy

The latest versions of these documents are maintained in the ISMS Documentation Register.

6. Roles and Responsibilities

Top Management: Provide leadership and commitment to information security; approve information security policies and objectives.

Information Security Team: Maintain the ISMS; monitor compliance and manage information security risks.

IT Team: Implement and operate technical security controls.

Department Heads: Ensure policy compliance within their departments.

Employees and Users: Comply with all information security policies; report security incidents or weaknesses.

Data Privacy Function: Oversee personal data protection requirements, privacy risk assessments, breach escalation, grievance handling and third-party personal data processing controls.

Procurement Team: Ensure that information security and confidentiality requirements are integrated into supplier onboarding, contracting, assessment and periodic review processes.

HR Team: Ensure completion of onboarding and annual information security awareness training and support disciplinary processes in case of policy violations.

Suppliers and Third Parties: Comply with Farmson's information security, confidentiality, privacy, access control and incident reporting requirements when accessing Farmson information assets or systems.

7. Compliance and Enforcement

Failure to comply with this policy or supporting policies may result in:

- Disciplinary action as per the Employee Disciplinary Process
- Restriction or revocation of access privileges
- Termination of employment or contract in severe cases

Additionally, suppliers and third parties that fail to comply with Farmson's information security, confidentiality or data protection requirements may also be subject to corrective action, access restriction, contract review, suspension or termination, depending on the severity of non-compliance.

Where required, significant information security or personal data incidents shall be escalated to customers, regulators or other relevant stakeholders in accordance with applicable laws, contracts and internal procedures.

8. Policy Review and Maintenance

This Information Security Policy shall be:

- Reviewed at least annually
- Reviewed following significant security incidents
- Updated due to changes in regulatory, legal, or business requirements, new systems or applications, significant audit findings, supplier-related security incidents, customer requirements or changes in the information security risk profile.
- The ISMS review shall include information security risks, incidents, audit findings, corrective actions, KPI performance, training completion, supplier security performance, data privacy risks and opportunities for continual improvement.

Approved versions shall be communicated to all relevant stakeholders.

9. Policy Application

This policy and its supporting policies are approved by top management and are mandatory. Questions or clarifications regarding this policy should be addressed to the immediate reporting manager or the Information Security Team.

10. Information Security Targets and KPIs

Farmson shall establish, monitor and review annual information security and data privacy targets to evaluate the effectiveness of the Information Security Management System. Performance against these targets shall be maintained through an Information Security KPI dashboard and reviewed by management at planned intervals.

The following annual targets shall be monitored:

1. Information Security and Data Privacy Training

Target: 100% of employees to complete information security and data privacy awareness training annually.

Target: 100% of new joiners to complete information security awareness training during onboarding.

2. Supplier and Third-Party Security

Target: 100% of critical suppliers and third parties with access to Farmson information assets, IT systems, confidential information, intellectual property, regulated records or personal data to undergo information security due diligence or assessment.

Target: Information security clauses to be included in contracts or agreements with relevant IT, cloud, data processing and critical service providers.

3. Audit and Corrective Action

Target: 100% of internal and external information security audit findings to be tracked through corrective action plans.

Target: Critical and major audit findings to be closed within defined timelines, unless formally risk accepted by management.

4. Management Review

Target: ISMS performance, information security risks, incidents, audit findings, corrective actions, supplier security performance and KPI performance to be reviewed by management at least annually.

5. Cybersecurity Performance / Maturity

Target: Farmson shall periodically monitor information security performance through internal KPI dashboards, external audit outcomes, ISO/IEC 27001 assessment/certification status, and cybersecurity maturity reviews, where applicable.

Performance against these targets shall be documented, reviewed and retained as evidence of continual improvement.