matrix pharma corp

INFORMATION SECURITY POLICY

Effective Date: 24th November 2025
Version 1.0

CONTENTS

1. Introduction

Information is one of the organisation's most valuable assets, and protecting it is critical to maintaining trust, ensuring compliance, and supporting long-term business goals. Safeguarding confidentiality, integrity, and availability isn't just a technical responsibility — it's a shared commitment across the entire organisation.

This Information Security Policy provides a clear framework for how we manage and protect our data. It outlines the principles, responsibilities, and controls that guide our approach to security, helping ensure that information is handled consistently, securely, and in alignment with regulatory and business requirements.

2. Applicability

This policy applies to all employees, contractors, and third-party personnel of Matrix Pharmacorp and its affiliates, and is enforceable across every site and location where the organization operates. Everyone who accesses or handles company information is expected to follow the principles and requirements outlined here.

3. Policy Statement

Matrix Pharma Corp is deeply committed to protecting the information entrusted to us. Every piece of data, every system, and every connection plays a role in keeping our operations secure, our people confident, and our partners assured. Security, integrity, and resilience are built into everything we do.

We ensure the confidentiality, integrity, and availability of information with disciplined rigor across every system, process, and interaction. Our approach combines strong controls, compliance with all relevant legal, regulatory, and contractual requirements, and a proactive mindset that stays ahead of emerging risks.

Information security is strengthened by the active ownership of every individual at Matrix, working together with a unified purpose. Through awareness, accountability, and continual improvement, we protect what matters most: our people, our partners, and the trust they place in us.

4. Goals

- Enhance the risk management framework to ensure all information security risks are identified, assessed, and managed within the organisation's defined risk acceptance criteria.

- Achieve and maintain 100% compliance with all applicable regulatory and contractual obligations.

5. Commitments

- Define, implement, and regularly evaluate controls to safeguard the confidentiality, integrity, and availability of information.
- Establish, implement, monitor, and continually improve the Information Security Management System in accordance with ISO principles.
- Periodically review information security objectives to ensure continued suitability and alignment with organisational goals.
- Ensure full compliance with all applicable legal, regulatory, and other information security requirements.
- Develop and maintain competency through structured training, awareness programs, and effective communication.
- Foster a consistent and disciplined information security environment that supports adherence to policies and continual improvement.

6. Oversight and Implementation

- Our Top Management holds overall responsibility for the strategic direction and oversight of this policy, ensuring that it aligns with our corporate values as well as all regulatory and contractual obligations.
- The Information Security Management Committee is responsible for the effective implementation of this policy by integrating information security considerations into business operations, decision-making processes, and corporate strategy. This includes defining action plans, allocating necessary resources, monitoring compliance, and driving continual improvement.
- To maintain clear accountability, designated members and the Information Security Forum oversee information security initiatives, conduct periodic assessments, and report progress to the Information Security Management Committee. Compliance with regulatory requirements and industry best practices is ensured through the Information Security Management System framework, internal audits, and ongoing engagement with relevant stakeholders.

7. Review and Amendments

This policy will be communicated to all employees and relevant stakeholders and is applicable to all organizational facilities. It will be reviewed periodically to ensure continued suitability, adequacy, and effectiveness. Any required amendments will be proposed and implemented as necessary.

8. POLICY NUMBER

Doc No: MPPL/IT/1/2025-2026
Department Issuing: IT
Pages: 3