SOLARA
Active Pharma Sciences

SOLARA ACTIVE PHARMA SCIENCES LIMITED

INFORMATION TECHNOLOGY & INFORMATION SECURITY POLICY

Document History		
Version	Status	Date
1.0	Obsolete	03.04.2023
2.0	Effective	01.01.2025
Next Revision Date: 01.01.2027		

Poorvank Purohit

Prepared by
Ameet Kumar
GM – Human Resources

Approved by
Poorvank Purohit
MD & CEO

Disclaimer:

This document (and any extract from it) may not be copied, paraphrased, reproduced, or distributed in any manner or form, whether by photocopying, electronically, by the internet, within another document or otherwise, without the prior written permission of Solara Active Pharma Sciences Ltd. (Solara). Further any quotation, citation, or attribution of this publication, or any extract from it is strictly prohibited without Solara’s written permission

Policy Statement:

Solara Active Pharma Sciences Limited is committed to ensuring the secure and controlled deployment of information, systems, processes, and technology to protect organizational assets and maintain operational security. This policy outlines principles and procedures to safeguard information and associated infrastructure from unauthorized access, breaches, and external threats.

Purpose:

To define guidelines that ensure secure information management and controlled usage of technology to enable Solara to operate securely while mitigating risks associated with information security threats.

Scope:

The policy is applicable to:

1. All Solara employees, including consultants, Contractors and trainees.
2. IT infrastructure, telecommunications systems, and equipment owned or leased by Solara.
3. Physical facilities supporting IT operations.

Failure to comply with this policy may result in termination of contracts or employment and other applicable consequences.

Objectives:

To protect Solara's information and systems, the company is committed to:

1. Preventing unauthorized access and disclosure of information.
2. Embedding information security in the company's culture through training and awareness.
3. Implementing a risk management approach to design, monitor, and improve controls.
4. Safeguarding personal information of employees, customers, and third parties.
5. Maintaining business continuity plans and adhering to regulatory and contractual requirements.

Responsibilities:

1. Information Security Office (ISO): Monitors and investigates information security breaches.
2. Employees & Contractors: Comply with policy guidelines and report incidents.
3. Management: Ensure implementation, review, and compliance with the policy.

Risk Assessment & Management:

A systematic assessment of security risks will guide the implementation of controls to mitigate potential threats.

1. Frequency: Risk assessment will be conducted annually as needed.
2. Areas of Focus:
   - 2.1. Business impact from security failures.
   - 2.2. Threats and vulnerabilities in information systems.
   - 2.3. Adequacy of current controls to address evolving risks.

3. Risk Categories:
   - 3.1. Organization of Information Security (e.g., internal organization, mobile devices).
   - 3.2. Asset Management (e.g., responsibility for assets, information classification).
   - 3.3. Access Control (e.g., user access management, system control).
   - 3.4. Cryptography (e.g., cryptographic controls, secure areas).
   - 3.5. Operations Security (e.g., malware protection, backups).
   - 3.6. Communication Security (e.g., network security management).
   - 3.7. Supplier Relationship Management (e.g., supplier service delivery).
   - 3.8. Incident Management (e.g., managing and improving responses to security incidents).

Information Security Policy Statement:

Solara shall:

1. Protect information from unauthorized access and disclosure.
2. Establish controls through risk assessment to manage and mitigate risks effectively.
3. Investigate breaches and ensure preventive measures.
4. Maintain a business continuity plan, including regular testing.
5. Review and update policies annually or as needed.

Compliance Areas:

Key compliance areas include:

1. Regulatory requirements and contractual obligations.
2. Data privacy and protection laws.
3. Industry standards for cybersecurity and information security.

Review & Administration:

1. This policy will be reviewed periodically to ensure relevance and alignment with changing business needs and regulations.
2. Amendments or withdrawals of this policy are at the discretion of the HR Department of Solara.

References:

- ISO 27001: Information Security Management Systems
- General Data Protection Regulation (GDPR)
- Industry Best Practices for Information Security
- Relevant Local and International IT Laws