SOLARA ACTIVE PHARMA SCIENCES LIMITED

INFORMATION TECHNOLOGY & INFORMATION SECURITY POLICY

Document History		
Version	Status	Date
1.0	Effective	03.04.2023
Next Revision Date: 03.04.2025		

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

Purpose:

The purpose of this policy is to set principles that aid the controlled deployment and usage of information and associated systems, processes and technology and in-turn enable Solara to operate in a secured manner.

Scope:

This policy is applicable to all Employees, third party contractors, information technology infrastructures, telecommunications systems, physical facilities and equipment owned or leased by Solara. Solara reserves the right to change, modify, add, or remove portions of this policy at any time. Failure to comply with this policy could result in consequences including, but not limited to, termination of contract or employment.

Procedure:

Information Security Policy Statement:

1. Solara shall ensure the following

    1.1. Information shall be protected from unauthorized access and unauthorized disclosure
    1.2. Information security controls shall be established, implemented, monitored and improved using a risk management approach
    1.3. All breaches of information security, actual or suspected, shall be reported to, and investigated by the Information Security Office (ISO)
    1.4. Privacy of personal information belonging to customers, employees and third-party individuals shall be safeguarded
    1.5. Regulatory and contractual requirements shall be identified and complied with
    1.6. Business continuity plan shall be documented, maintained and tested
    1.7. Information security policies shall be reviewed and updated on an annual basis or following significant changes in the Solara business environment

2. Information Security is embedded in the Solara's culture through periodic awareness and education regarding the ISMS to the employees.

Risk Assessment:

1. Security requirements are identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the business impact likely to result from security breaches and failures. Risk assessment technique can be applied to the whole organization, or only parts of it, as well as to individual information systems, specific system components or services where this is practicable, realistic and helpful. The Risk assessment should be conducted annually

2. Risk assessment is a systematic consideration of:

    2.1. The business impact likely to result from a security failure, considering the potential consequences of a loss of confidentiality, integrity or availability of the information and other assets.
    2.2. The realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities and the controls currently implemented.
    2.3. To ascertain that our current controls and practices are compliant to the evolving information risk landscape and provides us adequate protection from external threat actors

3. The results of this assessment shall help to guide and determine the individual risk and design and define various risk to bring out appropriate mechanism for managing and implementing controls to protect against risk. The below could be few areas of risk, should not be treated as an exhaustive list of risk.

4. **Potential Risk:**

4.1. Organization of Information Security
- 4.1.1. Internal Organization
- 4.1.2. Mobile devices and teleworking

4.2. Human Resource Security
- 4.2.1. Prior to Employment
- 4.2.2. During Employment
- 4.2.3. Termination or change of employment

4.3. Asset Management
- 4.3.1. Responsibility for Assets
- 4.3.2. Information classification
- 4.3.3. Media handling

4.4. Access Control
- 4.4.1. Business requirements of access control
- 4.4.2. User access management
- 4.4.3. User responsibilities
- 4.4.4. System and application access control

4.5. Acceptable use of Information Assets
- 4.5.1. General Use and Ownership

4.6. Cloud Security

4.7. Cryptography
- 4.7.1. Cryptographic controls
- 4.7.2. Secure areas
- 4.7.3. Equipment

4.8. Operations Security
- 4.8.1. Operational procedures and responsibilities
- 4.8.2. Protection from malware
- 4.8.3. Backup
- 4.8.4. Logging and monitoring
- 4.8.5. Controls of operational software
- 4.8.6. Technical vulnerability management
- 4.8.7. Information systems audit considerations

4.9. Communications Security
- 4.9.1. Network Security Management
- 4.9.2. Information Transfer

4.10. Security Acquisition, Development and Maintenance

4.10.1. Security requirements of information systems
4.10.2. Information security in supplier relationships
4.10.3. Test Data

4.11. Supplier Relationship
4.11.1. Information security in supplier relationships
4.11.2. Supplier Service delivery management

4.12. Information Security Incident Management
4.12.1. Management of information security incidents and improvements

4.13. Information Security Aspects of Business Continuity Management
4.13.1. Information Security Continuity
4.13.2. Redundancies

4.14. Compliance

Solara Management reserves the right to amend/ withdraw the policy at any time without assigning any reasons whatsoever. The utility and interpretation of this policy will be at the sole discretion of the HR Department.