ANUPAM RASAYAN INDIA LTD.

INFORMATION SECURITY POLICY

Information Security Management System Manual

Version 2

Internal

DOCUMENT INFORMATION SHEET		
TITLE : Information Security Policy		
PURPOSE & SCOPE: This Document contains the high level information security policy statements of ARIL, approved by Management , Published and communicated to all employees & relevant external parties		
Document No: ARIL/IT/1/V 2	Version No: 2	Issue Date: 1st Jan 2024

Table of Contents

1 Policy Statement

A detailed organizational asset inventory shall be maintained with owners assigned for all important assets to provide appropriate protection.

All Business information shall be classified and handled on the basis of its value, legal requirement, sensitivity and criticality to the organization.

2 Purpose and Objectives

The Purpose of this policy is to ensure management commitment towards information security and the ISMS.

3 Scope of the Policy

This Policy is directed towards the management of Anupam Rasayan India Ltd.

4 Responsibility for the Policy

Top Management of ARIL is responsible for supporting Information security initiatives by ensuring adequate resources and periodically reviewing the effectiveness of security measures.

5 High Level Information Security Policy

5.1 Information Security Management System Vision

Our Vision is to create a committed culture towards information protection and align Information Technology and Security activates with Anupam Rasayan India Ltd. Business processes in order to achieve the vision.

5.2 Information Security Management System Policy

"The ARIL's Information Security Policy is an explicit commitment to delivering high standards in information security management and it is integral to our approach for delivering superior business performance in all our operations. This policy supports our commitment to the well-being of our operations and assets."

In implementing this Information Security Policy, management of ARIL will:

- Identify and periodically assess the security threats arising from its business operations
- Develop and maintain an effective Information Security Management System.
- Accuracy of information assets and processing methods including all company's physical assets, personnel, corporate image and key business processes, from all forms of harm.
- Consider information security at all stages of planning.
- Mitigate or minimize risks by use of proactive and cost-effective measures and procedures.

- Encourage a positive commitment to information security by all levels of management by providing sufficient resources commensurate with the assessed risks.
- Record, analyse and investigate all reported security incidents and irregularities and develop improvements to prevent their re-occurrence.
- Introduce programs to develop information security awareness and responsibility among all staff and contractors.
- Ensure compliance with the policy through a process of education, review and audit.
- Develop policies, procedures, guidelines and provide awareness to users for implementation of the same.

6 Policy Implementation

6.1 Minimum Baseline Security Control Matrix

The requirements in the following table outline the minimum baseline security control
(MBSC) mechanisms that must be used for each information classification.

Security Objective	**Public**	**Internal**	**Confidential and Restricted**
Identification & Authentication	None	User IDs & Password	Users IDs & Its Password should not be share & with strong authentication.
Availability	Virus Scanning, Backup/Restore	Virus Scanning, Backup/Restore	Virus scanning, strong change control over system configuration, backup/restore
Confidentiality	None	None	Communications (all), and files on storage media shall be encrypted (whenever it is feasible) or password protected.

Printed Materials	None	Reasonable precautions to prevent access by non-employee	Storage in secure manner, E.g. secure area, Lockable enclosure

Security Objective	**Public**	**Internal**	**Confidential and Restricted**
Electronics documents	None	Storage on all drives	Storage on secure drives. Storage on shared drive without password protection for reading is prohibited. Password protection of documents preferred.
Email outside the organization	None	None	Email will be encrypted (whenever it is possible) Broadcast to distribution list is prohibited.
Conversations / Meetings	None	None	Active measures to prevent unauthorized parties from overhearing information and close control to limit information to as few persons as possible. Enclosed meeting areas. Public are prohibited. Avoid Public area e.g. elevators, hallways, cafeteria etc.
Computer screens	None	To prevent viewing by non-employees.	Viewing by unauthorized parties. Possible measures include physical location in a secure area, positioning of screen, and use of password protected screen saver (if possible)

Magnetic media, diskettes	None	None	Overwrite OR reformat

7 Protecting Data

7.1 All Key business data shall be assigned a data steward and access to this data monitored and controlled.

7.2 Secret & Confidential Documents shall not be left out on desks when not being used. Secret and confidential paper documents and computer media shall be stored in suitable locked cabinets or other forms of security furniture. Random checks may be made to check for confidential documents left unattended or unlocked.

7.3 When working on a computer located outside of an ARIL office, it is the responsibility of the user to ensure that the computer physically secure and that data cannot be accessed by third parties. Users should refer to ARIL IT Department for further information and guidelines about remote working.

7.4 Unwanted removable media such as CDs, tapes or USB memory devices, the hold confidential information shall be securely wiped or physically destroyed.

7.5 Users shall not modify/destroy information without proper authority.

8 Reporting Security Incidents

All IT Related security incidents shall be reported as quickly as possible to IT Service Desk in first instance. Line management should also be informed where appropriate. Non-IT related incidents shall be reported to the local information Protection office or Security officer.

ARIL IT Department

Information Classifications details

Classifications:	Internal
Information Owner:	Information Security Steering
Information Custodian:	Information Security Manager
Authorization List	All Employees, Contractors.
Declassify on:	Never