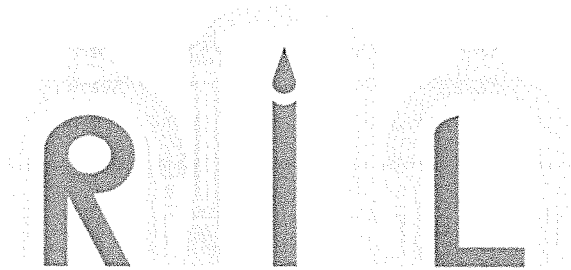




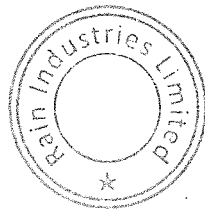
Rain Industries Limited

Information Technology and Cyber Security Policy



RAIN INDUSTRIES LIMITED

**Information Technology and Cyber Security
Policy**



RAIN INDUSTRIES LIMITED

CIN : L26942TG1974PLC001693

Regd. Office: Rain Center, 34, Srinagar Colony, Hyderabad – 500 073, Telangana State, India.

Tel: +91 40 4040 1234, Fax: +91 40 4040 1214, Website: www.Rain-industries.com

Email: secretarial@Rain-industries.com

Information Technology and Cyber Security Policy

1. Objective

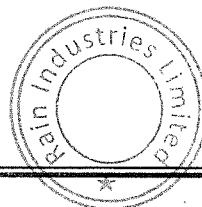
The objective of this Information Technology and Cyber Security is to ensure that “Due Care” is exercised in protecting information assets of Rain Industries Limited (hereafter referred to as “Rain” or “Organization”) and “Due Care” is defined as the cost-effective protection of information at a level appropriate to its business value. The value of the information assets can be quantified as the risk to Rain and if the confidentiality and/or integrity and/or availability are compromised.

The objective of the policy is –

- Demonstrate organization’s commitment to establish Information Technology and Cyber Security by establishing comprehensive management process throughout the organization.
- To convey management’s mission and vision for incorporating Information Technology and Cyber Security in the Organization’s culture
- To identify groups/teams and individuals responsible for implementation, maintenance, compliance, and improvement of Information Technology and Cyber Security
- To establish requirements for Rain employees to understand and adhere to Information Technology and Cyber Security Policies and Procedures.

Rain Information Technology and Cyber Security Management System Policy ensures that:

- Security of Rain assets is of paramount importance. Confidentiality, integrity, and availability of the assets shall be always maintained through controls that are adequate to the criticality of the asset, to protect the assets from all types of threats, whether internal or external, deliberate, or accidental.
- All forms of information (electronic/ print) on any medium will be classified and protected as per Information Technology and Cyber Security requirements.
- An Information Technology and Cyber Security framework shall be established for setting the objectives, Information Technology and Cyber Security roles and responsibilities.
- RAIN will carry out strategic business risk assessment at defined intervals in accordance with the risk assessment methodology and criteria for evaluation and acceptance of risks shall be defined.



- Any security incidents and infringement of policy, actual or suspected are reported, investigated by the designated Cybersecurity head and appropriate corrections and corrective action initiated.
- Awareness programs on Information Technology and Cyber Security are available to all employees and wherever applicable to third parties viz. subcontractor, consultants, vendors etc. and regular training imparted.
- The designated Chief Information Officer (“CIO”) is directly responsible for maintaining and for providing advice and guidance on the policy implementation. The IT Committee (“ITC”) is responsible for reviewing the policy according to the defined review process.
- The policy will be reviewed at periodic intervals (at least once in a year) – to check for its effectiveness, changes in technology, legal and contractual requirements, and business efficiency.
- The approved policy shall be communicated or made available to all employees and external parties having access to Rain information or information processing facilities.
- Policies and procedures are defined at department level to ensure protection of information assets and define objectives for continual improvement of ISMS.
- All location heads and Heads of Departments are directly responsible for implementing the policy within their Departmental areas and adherence by their staff; and
- It is the responsibility of all employees to adhere to the policy and the Management has all rights to act in case of its violation.

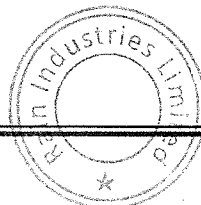
Need for ISMS

- Rain understands that information resources play a vital role in the conduct and success of business. Information and information resources must be protected throughout its life cycle. This ensures confidentiality, integrity and availability of the information captured, collected, processed, or stored on these resources. To protect Rain information resources, proper controls required to ensure compliance with internal and external regulations are put in place.

2. Scope

The Information Technology and Cyber Security policy applies to all Rain employees & employees of enabling functions including Human Resource, IT Department, Facilities, Finance, Legal, and Internal Audit at Rain regardless of position.

The policy shall also be applicable to all external/ third party personnel (i.e. vendors, third party resources, consultants, interns, contractors employed with Rain and clients/ customers visiting Rain offices who engage in work and have access to Rain information or information processing facilities). ISMS applies to all assets (i.e. physical assets, paper assets, people assets, information assets, site as an asset, software assets and services as an asset) at Rain Industries. The ISMS applies to all IT



technologies and services (i.e storage, backup, server hosting services, application services, cloud services, etc) that are delivered as an enabler to support Rain service delivery. Technology will also act as an enabler in implementing the Information Technology and Cyber Security controls across the organization. To support technology,

As a part of the ISMS the following departments are covered, supported externally by HR, Physical Security, Facilities, IT, Internal Audit:

- Data Centre Operations
- Network Operations
- Application Development and Testing

The Organizations ISMS shall be maintained as per the Statement of Applicability highlighting all the controls that are implemented and justifying the controls that are not implemented.

- **In Scope Location**

Rain shall develop, implement, maintain, and continually improve the documented ISMS for every office located at respective places within the context of Rain business activities and risk.

3. Responsibility

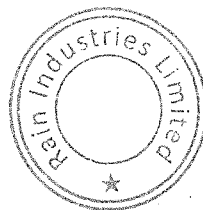
This policy states that Department and location heads are responsible for securing the information resources of Rain Industries. This policy also defines the authority, roles and responsibilities of Information Technology and Cyber Security and other groups, and personnel responsible for protecting Rain resources.

The Information Technology and Cyber Security organization structure at Rain shall consist of:

- Executive Vice President & Chair of the IT Committee (hereafter referred to as “ITC”)
- Members of ITC
- Chief Information Office
- Head – Information & Cyber Security
- Information Technology and Cyber Security /Cybersecurity team
- Global Internal Audit

4. Allocation of Information Technology and Cyber Security Responsibilities

- Roles and responsibilities shall be clearly defined and communicated to the identified functionaries of the Information Technology and Cyber Security organization; and
- The management shall ensure that requisite support is provided for the execution of ISMS in the organization.



5. Policy Statement

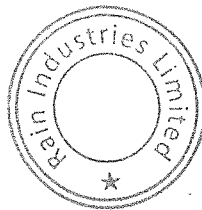
Information is an asset which, like other important business assets, has a value to the organization and consequently needs to be protected. Therefore, Rain recognizes its information assets as a significant and valuable resource. The Rain Information Technology and Cyber Security policy provides management direction and support to ensure protection of Rain information assets, and to allow access, use and disclosure of such information in accordance with appropriate standards and laws. The specific Information Technology and Cyber Security objectives for Rain and its enabling functions are:

- To develop and maintain an effective ISMS consisting of an Information Technology and Cyber Security policy, supporting procedures and a risk assessment framework.
- To identify all assets that directly or indirectly impact the client operations and understand their vulnerabilities and the threats through appropriate risk assessment.
- To comply with applicable laws and contractual obligations pertaining to Information Technology and Cyber Security and data privacy, for its client data and internal data; and
- To raise awareness of Information Technology and Cyber Security risks within Rain and create & maintain a security-conscious culture ensuring that all breaches of Information Technology and Cyber Security and suspected weakness are reported, investigated and adequate actions are taken.

- **Policy Framework**

Rain Information Technology and Cyber Security Policy is supported by detailed Information Technology and Cyber Security policies and procedures, implementation guidelines and templates. The Information Technology and Cyber Security procedures are derived from the policy statements and provide the details of necessary actions to achieve the objectives of the policy statement. The templates are derived from the detailed procedures and aim at facilitating the implementation of the Information Technology and Cyber Security Management System.

- **Policy Owner**
 - The ownership and responsibility for the maintenance of this Information Technology and Cyber Security policy lies with the CIO.
 - User must be contacted in the event of any questions on the contents of this policy, suggestions for improvements, specific security recommendations and any other areas relating to the security of systems, data, or information of Rain and all the enabling functions.



- **Policy Review and Approval**

This policy document shall be reviewed at least annually by the Leadership and Cybersecurity team or in events of any significant changes (i.e., change in operations, change in technology, regulatory changes, major security incidents) in the existing Information Technology and Cyber Security environment affecting policies and procedures. The policy owner will be responsible to make the changes to the policy document. The ITC will be responsible to approve the changes to the policy.

All changes to the policy shall be communicated by the cybersecurity team to all employees and third-party personnel through appropriate forums and channels.

- **Compliance**

- All employees, stakeholders and third-party vendors, contractors and consultants having access to Rain information and all the supporting processes of information processing facilities shall comply with the Information Technology and Cyber Security policy. All violation or any attempted violation of the Information Technology and Cyber Security policies shall result in disciplinary action to be taken by the ITC in consultation with human resources. Disciplinary action shall be consistent with the severity of the incident, as determined by an investigation department (in accordance with Rain Code of Conduct); and

- All violations of the Information Technology and Cyber Security policy must be reported to the respective Location/ Department Head (for all the supporting processes) and the cybersecurity team.

- **Exceptions**

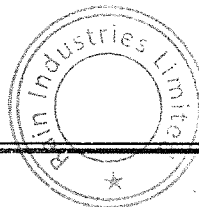
- Approval for exceptions or deviations from the policies, wherever warranted, will be provided only after an appropriate assessment of the risks arising out of providing the exception. This assessment will be conducted by the cybersecurity team. Exceptions will not be universal but will be agreed on a case-by-case basis, upon official request made by the asset owner. These may arise, for example, because of local circumstances, conditions or legal reason existing at any point of time. Exceptions to the Information Technology and Cyber Security Policy may have to be allowed at the time of implementation of these policies and guidelines or at the time of making any updates to this document or after implementation (ad-hoc).

All exceptions during implementation must be submitted by IT department to the ITC; and

- For any ad-hoc exception required by a User, a request for exception must be submitted by the user through formal channels to the ITC. This request must be approved by the User Department Head / asset owner.

- **Inquiries**

Any inquiries relating to policy, or the application of this policy shall be referred to the ITC.



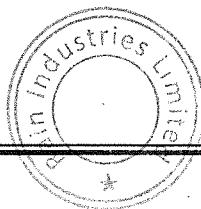
6. Management direction for Information Technology and Cyber Security

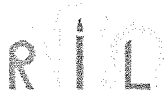
The management, consisting of the ITC, shall be accountable for enforcing the implementation of Rain Information Technology and Cyber Security policy. The location/ department heads along with the ITC shall be responsible for managing the overall Information Technology and Cyber Security for Rain Industries. All employees shall read, understand, and adhere to Rain Information Technology and Cyber Security policy. The Information Technology and Cyber Security policy for Rain shall be reviewed at least once in a year and at a time of any major change(s) in the existing environment affecting the policies and procedures. The review shall be conducted for assessing the following:

- Impact on the risk profile due to, but not limited to, the changes in information assets, deployed technology/ architecture and/ or legal requirements, emerging threat landscape; and
- Effectiveness in policies.

7. List of Policies

1. Access control policy
2. Anti-Malware Policy
3. Asset Management Policy
4. Change Management Policy
5. Clear Desk and Clear Screen Policy
6. Cloud Security Policy
7. Communication and Operation Policy
8. Compliance Policy
9. Configuration Management Policy
10. Continuity Management Policy
11. Cryptographic Control and Encryption Policy
12. Data Leakage Prevention Policy
13. Data Masking Policy
14. Data Privacy policy
15. Data Retention Policy
16. HR Security Policy
17. Information classification policy
18. Information Deletion - Disposal and Destruction Policy
19. Information Security Incident Management Policy
20. Information Technology and Cyber Security Policy
21. Logging and Monitoring Policy
22. Mobile Device and Teleworking Policy
23. Password Policy
24. Physical and Environmental security policy
25. Problem Management Policy
26. Secure Development Policy
27. Service Request and Incident management policy
28. Supplier Relationship Policy
29. Supplier Security Policy
30. System Acquisition, Development and Maintenance Policy





8. List of Procedures

1. Administrative Management Procedure
2. Backup and Recovery Procedure
3. Capacity Management Procedure
4. Event Management Procedure
5. Facilities and Datacentre Management Security Procedure
6. Infrastructure Change Management Procedure
7. ISMS Internal Audit Procedure
8. Network Security Procedure
9. Patch Management Procedure
10. Problem Management Procedure
11. Risk Management Procedure
12. Service Continuity Management Procedure
13. Service Desk Procedure
14. Service Request Management Procedure
15. Third-party Risk Management Procedure
16. Threat Intelligence Procedure
17. Web Filtering Procedure

9. Enforcement

Necessary disciplinary action will be taken based on the severity of the incident, it will deal case to case in coordination with HR Team and respective Department Head. Implementation of the policy will be verified during the internal audits and Management review meetings.

10. Confidentiality

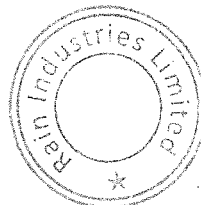
This document contains restricted confidential information pertaining to Rain Industries Limited. The access level for the document is specified above in the Document Details section. Employees and others must take steps to prevent intentional or accidental access outside the scope of access indicated.

11. Disclaimer

This document is confidential and is solely for the information of Rain and must not be used, circulated, quoted, or otherwise referred to for any other purpose, nor included or referred to in whole or in part in any document without Rain's prior written consent.

12. General

1. In case of any doubt with regard to any provision of the policy and also in respect of matters not covered herein, a reference to be made to the IT Committee/Chief Information Officer (CIO)/ IT Department. In all such matters, the interpretation & decision of the IT Committee shall be final.



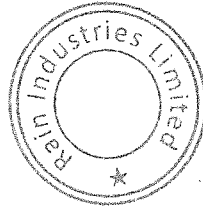


Rain Industries Limited

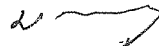
Information Technology and Cyber Security Policy

2. In the event of any conflict between the provisions of this Policy and of the Act or any other statutory enactments, rules, the provisions of such Act or statutory enactments, rules shall prevail over this Policy. Any subsequent amendment/modification in the Act and/or applicable laws in this regard shall automatically apply to this Policy.
3. Any or all provisions of the Policy may be amended with the approval of the Board of Directors.

By Order of the Board
for **Rain Industries Limited**



Place: Hyderabad
Date: August 06, 2024


N. Radhakrishna Reddy
Managing Director
DIN: 00021052