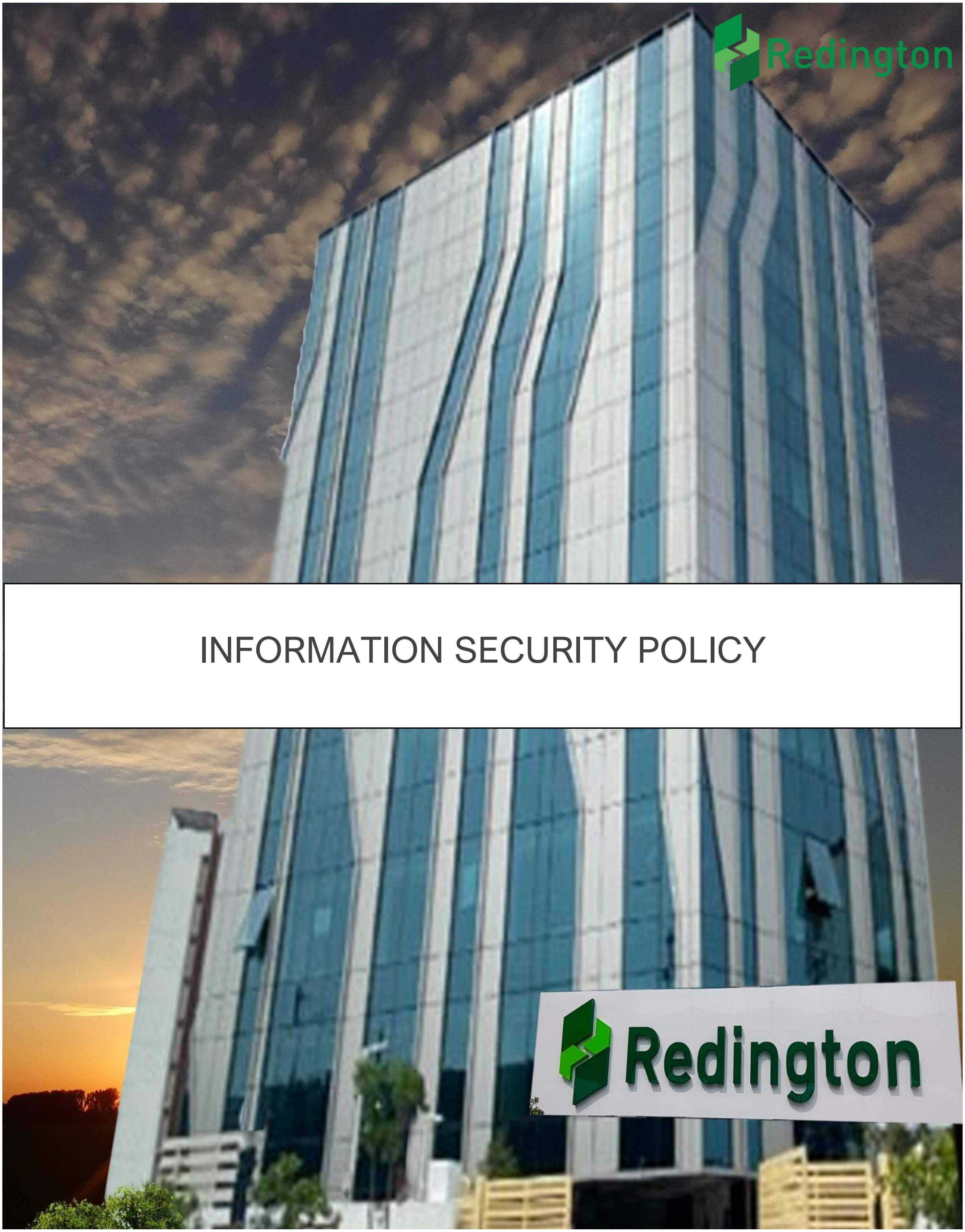

INFORMATION SECURITY POLICY

Document Control

Policy Owner:	Information Security Steering Committee
Policy Ref. No.:	RL_IND_ISMS_POL_01_2025
Approved By:	Pravin Kumar S
Approval Date:	04-April-2025
Version No.:	V 1.2
Version Date:	04-April-2025
Approver's Signature:	DocuSigned by: Pravin Kumar Sadasivam F127E8FD342B48C...
Information Classification	General Business

Change Log

Version No.	Document Creation, Review, Approval and Change Tracking	Actioned by (Name, Title, Department)	Action Date	Change Effective Date
1.0	Reviewed and approved the first release	Pravin Kumar S - CTO	23-05-2023	23-05-2023
1.1	Annual update and review	Pravin Kumar S - CTO	30-04-2024	30-04-2024
1.2	Reviewed and updated as per the 2022 version	Pravin Kumar S - CTO	04-04-2025	04-04-2025

Table of Contents

1. Introduction

Redington Group recognizes the importance of an Information Security Management System in reducing the impact of any breach of business-critical information.

To achieve this objective Redington Group has adopted the international standard for Information Security, ISO 27001:2022. This standard defines the requirements for an Information Security Management System (ISMS) based on the best international practices.

2. Purpose

The purpose of this policy is to demonstrate Redington Group top management's commitment with respect to the Information Security Management System by ensuring that the Information Security Policy is established. This policy is in compatibility with the strategic directions of Redington Group. This policy would provide guidance for ensuring the availability of necessary resources needed for ISMS and achievement of its intended outcome's. This policy also directs and supports Redington Group personnel to contribute to the effectiveness of the ISMS and promote continual improvement.

3. Policy

3.1 Information Security Requirements

Requirements for Information security shall be determined by understanding the interested parties and their requirements relevant to information security. The requirements of interested parties shall include Statutory, Regulatory, and contractual requirements.

Based on the requirements and the outcome of the risk assessment Redington group shall develop and implement policies and procedures to secure the information and information assets.

3.2 Information Security Principles

According to business needs, Redington Group Management has defined a set of information security principles to establish the security framework for Redington Group's information systems. Redington Groups information security principles are as follows:

Awareness: All staff shall be aware of the need for security of Redington Group information and must comply with the Corporate Information Security Policy, practices, guidelines and all relevant procedures.

Accountability: All Staff shall be accountable for the actions relating to the proper use and management of corporate information and corporate information systems.

Ethics: All staff should respect the legitimate interests of others. Information security should be implemented in a manner consistent with the values recognized by local society, the confidentiality of information and communication, the appropriate protection of personal information and transparency.

Multidisciplinary: Information security shall be achieved through the joint actions of the information owners, users and specialized security personnel. Decisions shall be reached after careful consideration of all related assessments and opinions in order to achieve the highest level of security.

Proportionality: Security mechanisms and controls applied on every information asset shall be proportional to the asset's value, the threats affecting the asset and the impact caused by a potential security violation.

Integration: Mechanisms, policies and security procedures shall be coordinated and integrated in an information security management system to establish a more effective security, while reducing cost and complexity.

Timeliness: When facing a security incident, the organization's personnel must act in a timely and coordinated manner using the official security incident handling procedure. With the appropriate administrative and technical security mechanisms in place, prevention or mitigation of future threats is achieved.

Equity: Security policy and controls that are applied throughout the organization must consider and not violate the rights of all parties involved in information processing.

Management Responsibility: Management staff shall ensure that the information security policies, practices, guidelines, and all relevant procedures are followed in their area of responsibility. In addition to that, management shall ensure that their staff is adequately trained in, understand, and adhere to the information security policies, practices, guidelines, and procedures.

Staff Responsibility: All Redington Group staff are responsible for the security of its information. The responsibilities of each staff member differ and shall be tailored according to their role.

Applicability: The information security policies are applicable to all Redington Group Information Technology (IT) organizational units. Subsidiaries, suppliers, contractors, service providers and any other third parties that Redington Group IT collaborates with, shall abide to all relevant security policies.

Incident Analysis: Suitable technological methods for logging, analysis, and correlation of security incidents with physical entities shall be implemented, so that such incidents can be identified timely, and if required, all possible security threats be investigated.

Incident Response: All staff shall immediately report all security incidents or weaknesses that they become aware of. The approved procedures for the investigation, escalation and handling of incidents shall be followed. All involved staff should act in a timely and co-operative manner so that security incidents can be prevented, identified, and appropriately handled.

Legislation: All staff shall comply with current legislation and regulations with regards to information security.

External Security: Wherever the security requirements surpass the external virtual boundaries of the organization, the necessary security responsibilities shall be determined, approved, and assigned.

Information owner: An Information Owner shall be designated for all information processed by Redington Groups information systems and IT infrastructure. The Information Owner is responsible for business activities which support information processing. The Information Owner is liable for the security of information for which he / she is responsible, even if he/she transfers his/her duties to specialized individuals or even if other trusted members are granted access for the processing and use of the information.

Access levels: Appropriate access levels to information and information systems shall be specified and maintained by information owners while access shall only be granted when there is a business need for it.

Information classification: Information Owners must classify their information as per the need for confidentiality, integrity, and availability. Information shall be protected according to its classification level during its processing, storage, and transmission.

Risk Assessment: Information security risk assessments shall be carried out so that possible threats and vulnerabilities are identified, acceptable risk levels are determined, and appropriate management and technical controls can be selected.

Security Approach: A multi-disciplinary approach shall be followed for the management of information security. Management and technical security controls should be integrated to create a coherent system for the management of information security.

Security lifecycle: Information Security shall be a fundamental element of all information systems developed or acquired by Redington Group so that security requirements are covered in a way that promotes client trust, compliance with legal and regulatory obligation, revenue creation and protection of Redington Group Information system assets. Information systems need to be designed, implemented, and connected with other systems, operated, administrated, and monitored according to Redington Groups approved policies, practices, guidelines, and procedures.

Connections: Connections with any third-party systems and networks shall not be implemented prior to an appropriate evaluation of possible security implications to Redington Groups business activities by information security department.

New Technologies: New technologies shall not be adopted for use, prior to an appropriate evaluation of possible security implications to Redington Groups business activities by information security department.

Audits: Periodic and ad-hoc audits shall be performed so compliance with the information security policies, practices, guidelines, and all relevant procedures is examined.

Reassessment: Existing management and technical controls shall be reviewed and reassessed periodically and if considered necessary appropriate modifications shall be applied.

Confidentiality: Access to information shall be provided only to those who are authorized for such access on a business “need to know” basis.

Integrity: Information shall be protected from alteration, i.e., protection of its accuracy and completeness.

Availability: Access shall be given to information upon demand by any authorized user.

3.3 Top Management Leadership and Commitment

Top management shall show leadership and commitment with respect to the information security management system by establishing information security objectives and policies as per the organization's strategic directions.

Management shall communicate the importance of an effective information security management system by meeting the requirements so that the intended outcomes are achieved. The information security requirements shall be integrated with the business processes.

Management shall provide the necessary resources needed for the information security management system and shall promote continuous improvement for the suitability, adequacy, and effectiveness of the information security management system.

The Head of Information Security shall have overall authority and responsibility for the implementation and management of the Information Security Management System, specifically:

a) The identification, documentation, and fulfilment of information security requirements
b) Implementation, management, and improvement of security risk management processes
c) Integration of security operational processes, procedures, and controls

d) Compliance with statutory, regulatory, and contractual requirements
e) Reporting to top management on performance and improvement

3.4 Framework for Setting Objectives

Security objectives will be defined based on a clear understanding of the business requirements and as an outcome of the management review process during which the views of relevant interested parties may be obtained.

The objectives shall consider the applicable information security requirements and results from risk assessment and treatment.

Those objectives shall be documented with the resources required, the person responsible and timelines for completion. Management shall review them by evaluating and monitoring performance.

3.5 Roles and Responsibilities

All information security roles shall be defined and allocated in accordance with information security policies. Responsibilities for the protection of individual assets and for carrying out specific information security processes should be identified. Responsibilities for information security risk management activities and for accepting residual risks should be defined.

Details of required Roles and Responsibilities for the information security management system are detailed in a separate document. Information Security Roles and Responsibilities.

3.6 Continual Improvement

Redington Group shall implement the following measures for continuous improvement.

a) Continuous improve the effectiveness of Information Security
b) Sustain ISO 27001 certification on a continual basis.
c) Increase the level of proactivity with regards to information security
d) Shall evaluate the information security performance and the effectiveness of the information security management system by monitoring and measuring. The results shall be analyzed and evaluated for improvements.
e) Conduct internal audits at planned intervals to provide information on whether it confirms the requirements of the information security management system and ISO 27001 standards.
f) Ideas for improvements may be obtained from any source including peers, special interest groups, employees, customers, suppliers, IT staff, risk assessments and service reports. Once identified they will be recorded and evaluated as part of management reviews.
g) Top Management review on monitoring and measurement, audit, nonconformities, corrective actions, and opportunities.

3.7 Approach to Managing Risk

A risk assessment and treatment process shall be implemented to address the risk and opportunities of Interested parties and their requirements.

A risk assessment will be done to identify the risks associated with the loss of confidentiality, integrity, and availability of information within the information security management system.

Risk assessments shall be reviewed annually or upon any significant change to business or systems. The risk assessment process will be carried out as per the Risk Management Framework. A risk register will be used for the assessment and treatment of risks.

Risk management will take place at several levels within the Information Security, including:

a) Management planning – risks to the achievement of information security objectives will be assessed and reviewed on a regular basis.
b) Information security and IT service continuity risk assessments
c) Assessment of the risk of changes via the change management process
d) As part of major projects to achieve business change e.g., new computer systems and services.

3.8 Auditing and Review

Redington group shall establish the following audit and review mechanisms:

a) Internal Audit shall be carried out at planned intervals to verify conformity to Redington Group's own information security management system requirements and/or ISO 27001 standards.
b) External audit against the standard by the registered certification body to be certified and for maintenance of certification.
c) A management review of adherence to policies and procedures.

3.9 Control of Records

Evidence of records is a requirement of the standards and key to meeting the audit requirements. Hence relevant records to show the working of controls are maintained.

3.10 Policies

Considering the security requirements of Redington Group the following information security policies have been framed based on a series of security principles. All information security policies are listed below:

1. Risk Management Policy
2. Security Incident Management Policy
3. Physical Security Policy
4. Human Resources Security Policy
5. Clear Desk and Clear Screen Policy
6. Asset Management Policy
7. Acceptable Use Policy
8. Information Transfer Policy
9. Information Security Continuity Policy
10. Backup Policy
11. Access Control Policy
12. Information Classification Policy
13. System Acquisition, Development and Maintenance Policy
14. Security in Project Management Policy
15. Malware Protection Policy
16. Cryptography Policy
17. IT Equipment Policy
18. Change Management Policy
19. Capacity Management Policy
20. Vulnerability Management Policy
21. Network Security Policy
22. Secure Development Policy
23. Compliance with Regulatory Requirement Policy

24. Password Management Policy
25. Teleworking and mobile device policy
26. Media handling Policy
27. Log Management Policy
28. Information Security Audit Policy
29. Supplier Management Policy
30. Information Security Review Policy
31. Cloud Security Policy
32. Threat Intelligence Policy

4. Cross References & Related Documents

The following documents support the Redington Group Information Security Policy:

- Information Security Roles and Responsibilities
- Risk management Framework
- All policies referred to above.
- ISO 27001:2022 – A.5

5. Review and Maintenance

To ensure that the Information Security Policy remains effective, Redington Group periodically reviews and updates it.

6. Filing and Distribution

This policy is published on the Redington Group GRC Portal

It is distributed to:

- Redington Group Employees
- Redington Partners
- Third Party Contractors
- Suppliers/vendors