| Approved By | Controlled By |
|---|---|
| HOD(C&IT) | CISO |

| | |
|---|---|
| Document Name | **Information Security Policy** |
| Document Version | **1.0** |
| Document ID | **ISMS/DOC/POLICY/14** |
| Security Classification | **Public** |
| Review Frequency | **Annually** |
| Date | **19.05.2025** |

## Document Change Record

### Version History:

| Sl. NO. | Version | Issue Date | Prepared By | Reviewed By | Approved By | Change Description |
|---|---|---|---|---|---|---|
| 1. | 1.0 | 19.05.2025 | Shweta Roy Sr. Mgr (C&IT)<br>19.05.2025 | A K Choudhry<br>CISO,<br>GM(C&IT)<br>19.05.2025 | Rajan Kumar CGM (C&IT)<br>19.05.2025 | Initial Release |

### Distribution List:

- C&IT Department
- ISMS Security Forum

## Notes:

- This is a controlled document under ISO 27001 ISMS. Unauthorized changes are prohibited.
- Ensure the most recent version is used at all times.
- All changes must be recorded in the Document Change Record section.

## Purpose

This policy defines the organization's approach to managing information security and establishes a framework for protecting the confidentiality, integrity, and availability of information assets. It aligns with ISO 27001:2022 requirements and serves as the foundation for the entire Information Security Management System (ISMS).

## Scope

This policy applies to all employees, contractors, third parties, and systems that access, process, store, or transmit organizational information, regardless of location or ownership.

### Policy Statement

- The organization is committed to:
  - Protecting the confidentiality, integrity, and availability of all information assets.
  - Complying with applicable legal, regulatory, and contractual requirements.
  - Managing information security risks through appropriate controls.
  - Continually improving the effectiveness of the ISMS.
- Management shall:
  - Provide leadership and commitment to information security.
  - Establish clear roles and responsibilities for information security.
  - Allocate sufficient resources to implement and maintain the ISMS.
  - Review the effectiveness of the ISMS at planned intervals.

### Information Security Framework

- Risk Management
  - Information security risks shall be:
    - Identified through a formal risk assessment process.
    - Evaluated based on potential impact and likelihood.
    - Managed through appropriate risk treatment options.
    - Documented and reviewed at regular intervals.
- Documentation and Records
  - The organization shall maintain:
    - Documented information required by ISO 27001:2022.
    - Documented information determined as necessary for ISMS effectiveness.
    - Records demonstrating conformance to requirements.
- Security Awareness
  - All personnel shall:
    - Receive information security awareness training.
    - Be informed of their information security responsibilities.
    - Be updated on changes to information security policies and procedures.

## Review and Improvement

- The Information Security Policy shall be:
    - Reviewed annually or when significant changes occur.
    - Updated to reflect changes in risk, technology, business objectives, or external requirements.
    - Approved by top management.
- The ISMS shall be subject to:
    - Regular internal audits.
    - Management reviews to ensure continued suitability and effectiveness.
    - Continuous improvement activities based on review findings.

## Compliance and Enforcement

- Compliance with this policy is mandatory for all personnel.
- Violations may result in disciplinary action, up to and including termination of employment or contract.
- Regular compliance monitoring will be conducted to verify adherence to this policy.

## Responsibilities

- Top Management:
    - Approve information security policies.
    - Provide strategic direction for information security.
    - Ensure integration of ISMS requirements into business processes.
- Information Security Officer:
    - Develop and maintain the ISMS.
    - Monitor and report on ISMS performance.
    - Coordinate information security activities.
- Department Managers:
    - Implement information security controls in their areas.
    - Ensure staff compliance with information security policies.
- All Personnel:
    - Comply with information security policies and procedures.
    - Report security incidents and vulnerabilities promptly.

**Policy Review:** This policy will be reviewed annually or after significant changes to ensure continued effectiveness and alignment with ISO 27001:2022 standards.

**END OF DOCUMENT**