Approved By	Controlled By
HOD(C&IT)	CISO

Document Name	**Information Security Objectives**
Document Version	**1.0**
Document ID	**ISMS/DOC/SO/01**
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) 19.05.2025	A K Choudhry CISO, GM(C&IT) 19.05.2025	Rajan Kumar CGM (C&IT) 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 document establishes and communicates the strategic information security objectives that align with our organization's business goals and ISO 27001:2022 requirements, ensuring measurable and achievable targets for our Information Security Management System.

Objective

To define, communicate, and monitor information security objectives that support the organization's strategic direction while ensuring continuous improvement of our information security posture and regulatory compliance.

Scope

This document applies to all components of the Information Security Management System (ISMS) across the organization, including all information assets, processes, personnel, and third-party relationships within the defined ISMS scope.

Strategic Information Security Objectives

1. Confidentiality Protection

- Maintain zero incidents of unauthorized information disclosure
- Achieve 100% compliance with data classification and handling procedures
- Ensure 100% implementation of access controls based on least privilege principle

2. System and Data Integrity

- Maintain zero tolerance for data corruption or unauthorized modification
- Achieve 100% integrity verification for critical business data
- Implement comprehensive change management with 100% authorization compliance

3. Information Availability and Business Continuity

- Achieve 99.9% system availability for critical business applications
- Maintain Recovery Time Objective (RTO) of less than 4 hours for critical systems
- Ensure Recovery Point Objective (RPO) of less than 1 hour for critical data
- Achieve 100% successful backup verification and restoration testing

4. Cyber security Resilience

- Maintain a malware-free environment with 99.9% effectiveness
- Achieve zero successful cyber attacks on critical infrastructure

- Complete quarterly vulnerability assessments with 100% critical vulnerability remediation within 30 days

5. Regulatory and Legal Compliance

- Maintain 100% compliance with applicable legal, regulatory, and contractual requirements
- Achieve zero legal penalties or sanctions due to information security breaches
- Complete annual compliance assessments with full remediation of identified gaps

6. Risk Management Excellence

- Maintain information security risk exposure below organizational risk appetite
- Complete annual comprehensive risk assessments covering 100% of ISMS scope
- Achieve 100% implementation of approved risk treatment plans within defined timelines

Measurable Security Performance Indicators

Category	Security Objective	Target 2025	Achieved 2024	Performance Metric Source	Measurement Frequency
Availability	ERP System Availability	100%	99.95%	SAP Early Watch Tools	Monthly
	Network Infrastructure Availability	100%	99.2%	Network monitoring dashboards	Monthly
	Building Management Systems	100%	100%	BMS (Building Management System) logs	Monthly
Incident Management	Security Incident Response Time	≤4 hours	No incidents reported		Per incident
	Security Incidents Resolved Successfully	100%	No incidents reported		Monthly
	Mean Time to Recovery (MTTR)	≤8 hours	No incidents reported		Per incident
Physical	Unauthorized	Zero	Zero	Access control	Monthly

PUBLIC

Security	Physical Access Incidents			system logs + CCTV audit	
	Asset Loss from Physical Threats	Zero	Zero	Asset management system + incident reports	Quarterly
Access Control	Privileged Account Reviews	100% completion	100%	EWA Reports	Quarterly
	Unauthorized Access Attempts	≤0.1% of total access	0.01%	SAP Logs	Monthly
Vulnerability Management	Critical Vulnerability Remediation	100% within 30 days	85%	Honeycomb reports/CERT-in CSK	Monthly
	Vulnerability Assessment Coverage	100% of systems	98%	Asset inventory vs. scan coverage reports	Quarterly
	Security Patch Compliance	≥98%	96%	WSUS/SCCM patch management reports	Monthly
Business Continuity	Backup Success Rate	100%	99.8%	Backup software monitoring (Veeam/NetBackup)	Daily
	Disaster Recovery Test Success	100%	100%	DR test execution reports	Semi-annually
	Data Recovery Capability Verification	100%	100%	Restore test documentation	Quarterly
Compliance	Policy Compliance Assessment	≥98%	98%	Audit reports	Quarterly
	Training Completion Rate	100%	97%	L&D reports	Annually
	Audit Finding Closure Rate	100% within SLA	100%	Audit management system tracking	Per audit
Threat Management	Threat Intelligence Integration	100% coverage	90%	Honeycomb reports/CERT-in CSK	Monthly
	Security Monitoring	24/7/365	99.7%	Monitoring tool uptime	Continuous

	Coverage				
	False Positive Rate	≤5%	2%	Analyst feedback	Monthly

Performance Calculation Methodologies

Availability Metrics

- **Formula:** (Total Time - Downtime) / Total Time × 100
- **Data Sources:**
  - System uptime logs from monitoring tools
  - Scheduled maintenance windows (excluded from calculation)
  - Incident duration records

Incident Response Metrics

- **Response Time Calculation:** Time from incident detection/reporting to initial response
- **Resolution Rate:** (Incidents Resolved / Total Incidents) × 100
- **MTTR Calculation:** Total downtime for all incidents / Number of incidents

Access Control Metrics

- **Review Completion:** (Completed Reviews / Scheduled Reviews) × 100
- **Unauthorized Access Rate:** (Failed Access Attempts / Total Access Attempts) × 100
- **Data Sources:** Authentication logs, failed login attempts, access violation reports

Vulnerability Management Metrics

- **Remediation Rate:** (Critical Vulnerabilities Fixed within SLA / Total Critical Vulnerabilities) × 100
- **Coverage Calculation:** (Systems Scanned / Total Systems in Inventory) × 100
- **Patch Compliance:** (Systems with Latest Patches / Total Systems) × 100

Business Continuity Metrics

- **Backup Success:** (Successful Backups / Total Backup Jobs) × 100
- **Recovery Test Success:** (Successful Recovery Tests / Total Tests Performed) × 100

Compliance Metrics

- **Compliance Score:** Weighted average of control implementation across all policy areas

- **Training Completion:** (Employees Completed Training / Total Employees Required) × 100
- **Audit Finding Closure:** (Findings Closed within SLA / Total Findings) × 100

Implementation Framework

Resource Requirements

- **Human Resources:** Information Security Team, IT Operations, and designated Security Champions across business units
- **Technology:** Security monitoring tools, vulnerability scanners, backup systems, and incident response platforms
- **Financial:** Budget allocation for security tools, training, assessments, and incident response capabilities
- **Training:** Regular security awareness programs and specialized technical training for security personnel

Roles and Responsibilities

- **Chief Information Security Officer (CISO):** Overall accountability for ISMS objectives achievement
- **Information Security Team:** Day-to-day implementation and monitoring of security controls
- **Business Unit Managers:** Ensuring compliance within their respective areas
- **All Employees:** Adherence to information security policies and prompt incident reporting
- **Executive Management:** Strategic support and resource allocation

Implementation Timeline

- **Phase 1 (Months 1-3):** Baseline assessment and gap analysis
- **Phase 2 (Months 4-9):** Implementation of priority controls and processes
- **Phase 3 (Months 10-12):** Full deployment and optimization
- **Ongoing:** Continuous monitoring, measurement, and improvement

Monitoring and Review

- **Monthly:** Operational metrics review and dashboard updates
- **Quarterly:** Detailed performance analysis and trend identification
- **Semi-annually:** Objective relevance and target adjustment review
- **Annually:** Comprehensive ISMS objectives review and strategic alignment assessment

Continuous Improvement

The organization is committed to the continuous improvement of information security objectives through:

- Regular performance monitoring against established targets
- Integration of lessons learned from security incidents and near-misses
- Incorporation of emerging threats and technological changes
- Alignment with evolving business requirements and regulatory changes
- Benchmarking against industry best practices and standards

Communication and Awareness

These information security objectives will be communicated to all relevant stakeholders through:

- Annual security awareness training programs
- Regular security bulletins and updates
- Integration into employee performance objectives
- Management review meetings and board reporting
- Public commitment statements where appropriate

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

END OF DOCUMENT