Approved By	Controlled By
HOD(C&IT)	CISO

Document Name	**Statement of Applicability**
Document Version	**1.0**
Document ID	**ISMS/DOC/SOA/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.

Introduction

This Statement of Applicability (SoA) documents the controls from ISO/IEC 27001:2022 Annex A that are applicable to the Information Security Management System (ISMS) of the Computer & Information Technology Department. This SoA defines the scope of implementation and justifies the inclusion or exclusion of specific controls based on risk assessment results and organizational requirements.

Scope

The scope of this ISMS covers:

- All information assets managed by the Computer & Information Technology Department
- IT infrastructure including hardware, software, networks, and supporting technologies
- Operational processes and procedures related to information security
- All locations where departmental operations are conducted

Controls Implementation

A.5 Organizational Controls

Control ID	Control Name	Applicable (Y/N)	Implementation Status	Justification
A.5.1	Information security policies	Y	Implemented	Required to establish management direction and support for information security
A.5.2	Information security roles and responsibilities	Y	Implemented	Essential for clear accountability and governance
A.5.3	Segregation of duties	Y	Implemented	Prevents unauthorized or unintentional modification or misuse of assets
A.5.4	Management responsibilities	Y	Implemented	Ensures senior management commitment to security objectives
A.5.5	Contact with authorities	Y	Implemented	Required for incident reporting and compliance purposes

A.5.6	Contact with special interest groups	Y	Partially Implemented	Needed to maintain awareness of emerging threats and best practices
A.5.7	Threat intelligence	Y	Implemented	Critical for proactive security measures
A.5.8	Information security in project management	Y	Implemented	Ensures security is considered throughout project lifecycles
A.5.9	Inventory of information and other associated assets	Y	Implemented	Fundamental for asset protection and management
A.5.10	Acceptable use of information and other associated assets	Y	Implemented	Defines boundaries for proper use of organizational assets
A.5.11	Return of assets	Y	Implemented	Prevents information leakage when staff leave
A.5.12	Classification of information	Y	Implemented	Enables appropriate protection levels based on sensitivity
A.5.13	Labelling of information	Y	Implemented	Supports handling of information according to its classification
A.5.14	Information transfer	Y	Implemented	Protects information during transfer between entities
A.5.15	Access control	Y	Implemented	Essential for preventing unauthorized access
A.5.16	Identity management	N	Not Implemented	A centralized identity management system is not in place; however, identity controls are implemented at the application, database, and Active Directory (AD) levels. Each system manages access independently, ensuring adequate security. The organization recognizes the need for unified identity management and is evaluating options to integrate access control across systems.

A.5.17	Authentication information	Y	Implemented	Ensures secure access verification
A.5.18	Access rights	Y	Implemented	Controls what users can access
A.5.19	Information security in supplier relationships	Y	Implemented	Addresses third-party risks
A.5.20	Addressing information security within supplier agreements	Y	Implemented	Formalizes security requirements for suppliers
A.5.21	Managing information security in the ICT supply chain	Y	Implemented	Addresses specific risks in technology supply chains
A.5.22	Monitoring, review and change management of supplier services	Y	Implemented	Ensures ongoing compliance with security requirements
A.5.23	Information security for use of cloud services	Y	Implemented	Addresses specific cloud security considerations
A.5.24	Information security incident management planning and preparation	Y	Implemented	Essential for incident response readiness
A.5.25	Assessment and decision on information security events	Y	Implemented	Ensures proper evaluation of security events
A.5.26	Response to information security incidents	Y	Implemented	Provides framework for incident handling
A.5.27	Learning from information security incidents	Y	Implemented	Enables continuous improvement

A.5.28	Collection of evidence	Y	Implemented	Supports investigation and legal proceedings if needed
A.5.29	Information security during disruption	Y	Implemented	Ensures security is maintained during business disruptions
A.5.30	ICT readiness for business continuity	Y	Implemented	Ensures systems can continue or recover during disruptions
A.5.31	Legal, statutory, regulatory and contractual requirements	Y	Implemented	Ensures compliance with applicable requirements
A.5.32	Intellectual property rights	Y	Implemented	Protects organizational intellectual assets
A.5.33	Protection of records	Y	Implemented	Ensures integrity and availability of important records
A.5.34	Privacy and protection of PII	N	Not Implemented	A formal privacy framework is not yet implemented; however, basic measures to protect PII are in place through application-level controls, secure access, and limited data collection. The organization currently does not process large volumes of PII, and data handling is limited to internal purposes. A structured approach for privacy management, including data minimization, consent, and retention policies, is under consideration for future implementation to ensure full compliance with privacy regulations.
A.5.35	Independent review of information security	Y	Implemented	Provides objective assessment of security controls
A.5.36	Compliance with policies, rules and standards for	Y	Implemented	Ensures internal compliance

	information security			
A.5.37	Documented operating procedures	Y	Implemented	Provides clear guidance for secure operations

A.6 People Controls

Control ID	Control Name	Applicable (Y/N)	Implementation Status	Justification
A.6.1	Screening	Y	Implemented	Ensures personnel meet security requirements before employment
A.6.2	Terms and conditions of employment	Y	Implemented	Formalizes security responsibilities for employees
A.6.3	Information security awareness, education and training	Y	Implemented	Essential for building security culture and knowledge
A.6.4	Disciplinary process	Y	Implemented	Addresses violations of security policies
A.6.5	Responsibilities after termination or change of employment	Y	Implemented	Ensures continued security after employment changes
A.6.6	Confidentiality or non-disclosure agreements	Y	Implemented	Protects sensitive information through legal means
A.6.7	Remote working	Y	Implemented	Addresses specific risks of remote work arrangements
A.6.8	Information security event reporting	Y	Implemented	Enables timely reporting of security events

A.7 Physical Controls

Control ID	Control Name	Applicable (Y/N)	Implementation Status	Justification
A.7.1	Physical security perimeters	Y	Implemented	Prevents unauthorized physical access
A.7.2	Physical entry	Y	Implemented	Controls access to

				sensitive areas
A.7.3	Securing offices, rooms and facilities	Y	Implemented	Protects work areas from unauthorized access
A.7.4	Physical security monitoring	Y	Implemented	Enables detection of unauthorized physical access
A.7.5	Protecting against physical and environmental threats	Y	Implemented	Addresses non-human threats to physical infrastructure
A.7.6	Working in secure areas	Y	Implemented	Ensures security in high-sensitivity locations
A.7.7	Clear desk and clear screen	Y	Implemented	Prevents exposure of sensitive information
A.7.8	Equipment siting and protection	Y	Implemented	Protects hardware from physical threats
A.7.9	Security of assets off-premises	Y	Implemented	Addresses risks when assets are outside organizational premises
A.7.10	Storage media	Y	Implemented	Ensures proper handling of removable media
A.7.11	Supporting utilities	Y	Implemented	Ensures availability of power and other utilities
A.7.12	Cabling security	Y	Implemented	Protects network and power cables
A.7.13	Equipment maintenance	Y	Implemented	Ensures continued availability and integrity of equipment
A.7.14	Secure disposal or re-use of equipment	Y	Implemented	Prevents data leakage from disposed or reused equipment

A.8 Technological Controls

Control ID	Control Name	Applicable (Y/N)	Implementation Status	Justification
A.8.1	User endpoint	Y	Implemented	Secures devices used by

	devices			employees
A.8.2	Privileged access rights	Y	Implemented	Controls high-level system access
A.8.3	Information access restriction	Y	Implemented	Limits access based on need-to-know
A.8.4	Access to source code	Y	Implemented	Protects critical intellectual property
A.8.5	Secure authentication	Y	Implemented	Ensures proper identity verification
A.8.6	Capacity management	Y	Implemented	Ensures system availability
A.8.7	Protection against malware	Y	Implemented	Prevents malware infections
A.8.8	Management of technical vulnerabilities	Y	Implemented	Addresses system vulnerabilities
A.8.9	Configuration management	Y	Implemented	Ensures secure system configurations
A.8.10	Information deletion	Y	Implemented	Ensures proper data removal
A.8.11	Data masking	N	Not Implemented	Data masking is not implemented organization-wide; however, access to sensitive data is restricted through role-based access controls at the application and database levels. Since there is currently no exposure of production data to non-authorized personnel or non-production environments, the risk is considered low. Implementation of data masking for test environments and user interfaces is planned as part of the data protection enhancement roadmap.
A.8.12	Data leakage prevention	Y	Implemented	Prevents unauthorized data exfiltration
A.8.13	Information backup	Y	Implemented	Ensures data availability
A.8.14	Redundancy of	Y	Implemented	Provides system availability

	information processing facilities			during failures
A.8.15	Logging	Y	Implemented	Records security-relevant events
A.8.16	Monitoring activities	Y	Implemented	Enables detection of security violations
A.8.17	Clock synchronization	Y	Implemented	Ensures accuracy of security logs
A.8.18	Use of privileged utility programs	Y	Implemented	Controls high-risk system tools
A.8.19	Installation of software on operational systems	Y	Implemented	Controls changes to production systems
A.8.20	Networks security	Y	Implemented	Protects network infrastructure
A.8.21	Security of network services	Y	Implemented	Ensures security of network-based services
A.8.22	Segregation of networks	Y	Implemented	Isolates networks based on sensitivity
A.8.23	Web filtering	Y	Implemented	Controls web-based threats
A.8.24	Use of cryptography	N	Not Implemented	A formal cryptographic policy is not implemented; however, SSL/TLS is used to secure data in transit for web-based applications and portals. Other cryptographic measures, such as encryption for data at rest, are not yet applied consistently across systems. Access controls and network segmentation are currently used to safeguard sensitive data. The organization is planning to implement comprehensive cryptographic controls in alignment with data classification and risk levels.
A.8.25	Secure development life cycle	Y	Implemented	Ensures security throughout application development

A.8.26	Application security requirements	Y	Implemented	Defines security requirements for applications
A.8.27	Secure system architecture and engineering principles	Y	Implemented	Ensures security in system design
A.8.28	Secure coding	Y	Implemented	Prevents security vulnerabilities in code
A.8.29	Security testing in development and acceptance	Y	Implemented	Validates security controls
A.8.30	Outsourced development	N	Not Implemented	This control is not applicable as all software development activities are carried out internally by authorized employees. No development work is outsourced to third parties, thereby minimizing risks related to external development and third-party access to source code or sensitive information.
A.8.31	Separation of development, test and production environments	Y	Implemented	Prevents production impacts from development
A.8.32	Change management	Y	Implemented	Controls system changes
A.8.33	Test information	Y	Implemented	Protects test data
A.8.34	Protection of information systems during audit testing	Y	Implemented	Minimizes impact of security testing

Risk Assessment Methodology

The risk assessment methodology used to determine the applicability and implementation of controls follows ISO 27005 guidelines and includes:

- Asset identification and valuation
- Threat and vulnerability identification
- Risk analysis and evaluation

- Risk treatment planning
- Residual risk acceptance

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