AUDIT REPORT

For

SarthhakAI Private Limited

Address: B013, Raheja Atlantis, Sector 31, Gurugram, Haryana, 122001, India

Issue Date: December 30, 2025

Reviewed By:
Accorp Partners Cert Inc.
26500 Agoura Road Suite 207
Calabasas CA 91302, USA

Email: info@accorppartners.com
Web: https://www.accorppartners.com/

Table of Contents

1. Audit Summary:

Name of Organization	SarthhakAI Private Limited			
Address	B013, Raheja Atlantis, Sector 31, Gurugram, Haryana, 122001, India			
Additional Sites If any	NA			
Contact Person	Satvik Kalra	**Designation**	CEO	
Email Id	satvik@sarthhakai.com			
Scope of Certification	The Information Security Management System applies to bodh scientific™, an AI-native SaaS platform with the support functions of IT Infrastructure, Human Resources and Legal to ensure secure platform operations, governance and compliance. This is as per the latest Statement of Applicability (SoA) version 1.0.			
Standard and Exclusion(s), If any	Physical Security Controls and Outsourced Development	**No. of Personnel's**	5	**Excluded Control:** 8.19, 8.30 and 7.1 - 7.14

2. Requirements for Scheme (ISO 27001)

Requirements	Details/References
Updated statement of Applicability	The Statement of Applicability document confirms the requirements with proper descriptions. Status of control implementation is recorded. Justification of inclusion and exclusion is provided.
Justification for any exclusion	Physical Security Controls have been excluded as physical security is out of scope for the organization. Control A.8.30 is excluded as there are no software development activities outsourced.
Risk Assessment & Risk Treatment Plan	Risk assessment methodology is documented. Risk assessment and treatment is documented. Risk ownership is assigned. Risk treatment and acceptance criteria is defined. SoA controls are mapped to risk treatment.
Internal Audit Summary Report	Internal audit process is documented. Audits are conducted annually as per the documented process. Annual Audit calendar is maintained. The audit was conducted by an external consultant on December 16, 2025. RCA and corrective actions in any, are documented.
Minutes of MRM	Management review was done on December 17, 2025. Has covered topics as per clause 9.3.

3. Audit Objectives

a) to confirm that the client adheres to its policies, objectives, and procedures

b) top management leadership and commitment to information security policy and the information security objectives.

c) documentation requirements listed in International Standard.

d) assessment of information security-related risks and that the assessments produce consistent, valid and comparable results if repeated.

e) determination of control objectives and controls based on the information security risk assessment and risk treatment processes.

f) information security performance and the effectiveness of the ISMS, evaluating against the information security objectives;

g) correspondence between the determined controls, the Statement of Applicability, and the results of the information security risk assessment and risk treatment process and the information security policy and objectives.

h) implementation of controls (As per the Scheme), taking into account the external and internal context and related risks, the organization's monitoring, measurement, and analysis of information security processes and controls, to determine whether controls are implemented and effective and meet their stated information security objectives.

i) programs, processes, procedures, records, internal audits, and reviews of the ISMS effectiveness to ensure that these are traceable to top management decisions and the information security policy and objectives.

FOR ISMS:

- To obtain documentation on the design of the ISMS covering the documentation required as per ISO 27001:2022

- To obtain sufficient information on the management system in the context of the client's organization, risk assessment and treatment (including the controls determined) information security policy, and objectives

4. Audit Methodology

The audit has been conducted on the basis of the client management system by ACCORP PARTNERS. The audit is being based upon the verification of relevant policies, procedures, and evidence of the controls implemented.

5. Audit Summary

Accorp Partners has conducted an audit of the Information Security Management System as per the requirements of ISO 27001:2022 and confirmed the following:

6. Findings

Non-conformities

S.No	Non-conformities (NC)	Type of NC	Relevant Clause/Control Reference
1.	NIL		

Opportunities for Improvement

S.No	Opportunities for Improvement (OFI)	Relevant Clause/Control Reference
1.	MDM tool can be considered for control of Endpoint devices.	A.8.1
2.	Access revocation completion date can be documented for better tracking.	A.5.18

Positive Observations

S.No	Positive Observations	Relevant Clause/Control Reference
1.	Verified the BCP DR drill report dated December 06, 2025 and noted that test was conducted.	A.5.30
2.	Verified with the latest vulnerability assessment /penetration test report performed on December 04, 2025 and determined that VA/PT are carried out periodically and that vulnerabilities were closed.	A.8.8
3.	Verified that AWS CloudWatch has been configured for capacity monitoring and alerts are being generated.	A.8.6
4.	Verified that AWS Security Groups has been setup for Managing incoming and outgoing connection settings.	A.8.20
5.	Verified that sampled employee Rxxxxxh joined on May 30, 2025 screening was done with relevant laws and rules.	A.6.1
6.	Verified that sampled candidate Rxxxxxh Sxxxxxxxxv left the organization on July 24, 2025 and respective accounts access were taken in accordance with relevant laws and regulations.	A.6.5
7.	Positive - GRC Platform is being utilized for ISMS awareness training where quiz is also present for training effectiveness.	7.3

7. Audit Result

Based on the evidence presented and evaluated by us, SarthhakAI Private Limited has been recommended for ISO 27001:2022 Certification.

Based on the verification of submitted corrective action plan, SarthhakAI Private Limited has been recommended for ISO Certification.

Report Prepared By: Venu K

Report Reviewed By: Ram K

Audit Plan

Date & Time	Audit Focus / Clauses
December 23, 2025 to December 30, 2025	• CISO and Top Management • HR and Training • Operations - Helpdesk • IT infrastructure • Application Development • Operations – Incident Management, Change management • SOA, Supplier relationships and ISMS, HR • BCP Plan, Legal, Internal Audit and MRM • Risk Assessment and Continual Improvement

Audit Notes

Clause No.	Clause Description	Stage I - Audit Notes (Evidences, Observation & Findings)	Stage II / SA / RA / Other - Audit Notes (Evidences, Observation & Findings)
4.1.	Context of the organization	Organisation has identified and documented the context of the organization in the ISMS Clause Requirements, v2.0	Context is clearly understood by relevant stakeholders. Evidenced through interviews and documents. Implementation reflects the documented context.
4.2.	Understanding the needs and expectations of interested parties	Organisation has identified and documented the needs and expectations of interested parties in the ISMS Clause Requirements, v2.0	Stakeholders interviewed were aware of their responsibilities. Evidence of communication and review available. Register is current and accessible.
4.3.	Determining the scope in which MS is implemented	Organisation has identified and documented the Scope of the ISMS in the ISMS Clause Requirements, v2.0	Scope is well-defined and matches actual operations. No inconsistencies found during physical and logical walkthroughs.
4.4.	Management system and its processes	Organisation has identified and documented the processes and their interactions pertaining to requirements of the ISO 27001:2022 standard in the ISMS Clause Requirements, v2.0	Processes are effectively implemented. Evidenced by process owners' awareness, control documents, and consistent outputs.
5.1.	Leadership and commitment	Organisation has identified and documented Leadership and commitment in the ISMS Clause Requirements, v2.0. The Top Management of the company recognizes and ensures effective implementation, and maintenance of Information Security.	Strong leadership commitment observed. ISMS activities receive necessary resources. Top management actively reviews ISMS performance.
5.2.	Policy	The policy is communicated to employees. Communication is done during onboarding, annual	Information Security Policy is available, communicated, and understood. Verified during staff

		refresher training, and periodic mailers. The ISMS scope, security policy, and objectives are documented and communicated. Organisation has identified and documented Policy in the ISMS Clause Requirements, v2.0	interviews and training records.
5.3.	Responsibilities and authorities	The CISO and top management team have participated in the Sr. management discussion. The management team has a clear vision for the ISMS. Adequate resources are committed. The ISMS organization structure is defined, Resources across the organization are part of the ISMS org structure. Roles, responsibilities, and authorities are defined. Security initiatives are taken on priority and are aligned with the business strategy. Strong commitment from Sr. management was evident during the course of the audit. Organisation has identified and documented Responsibilities and authorities in the ISMS Clause Requirements, v2.0	Roles and responsibilities are clearly defined and effectively delegated. Organizational structure reflects security governance.
6.1.	Actions to address risk and opportunities	The risk assessment methodology is documented. Risk assessment and treatment are documented. Risk ownership is assigned. Risk treatment and acceptance criteria are defined. SoA controls are mapped to risk treatment. Organisation has identified and documented Actions to address risk and opportunities in the ISMS Clause Requirements, v2.0.	Risk register is maintained and updated. Evidence of periodic reviews and risk treatment activities. Risk ownership is actively managed.

6.2.	Objectives and planning to achieve them	ISMS objectives are defined at the org level and cascaded to functions. SOA controls identified. The status of control implementation is recorded. Physical Security Controls have been excluded as the Physical security is out of scope for the organization and A.8.30 control is excluded as there is no s/w development activities outsourced. Justification of inclusion and exclusion is provided. Organisation has identified and documented Information security objectives and planning to achieve them in the ISMS Clause Requirements, v2.0.	ISMS Objectives are monitored, and linked to metrics. Evidence of review during management meetings. Progress is tracked via dashboards.
7.1.	Resources	Organisation has determined and provided resources that are needed for the establishment, implementation, maintenance, and improvement of the Information Security Management System which is documented in the ISMS Clause Requirements, v2.0.	Resources (human, technical, and financial) are adequate and appropriately allocated. No gaps observed during the audit.
7.2.	Competence	Skill matrix is available for key roles and Organisation has documented Competence in the ISMS Clause Requirements, v2.0.	Competency mapping and training plans are in place. Evidence of periodic skill assessment and training effectiveness review.
7.3.	Awareness	Awareness is provided to the employees. Awareness training provided during induction and yearly refresh training. Awareness trainings are made available in the LMS system. All employees have completed the training. Organisation has identified and documented Awareness in the ISMS Clause Requirements, v2.0.	Staff interviews confirm understanding of ISMS policies and risks. Awareness is maintained through regular training and email campaigns.
7.4.	Communication	Communication process and	Communication channels are

		a document control policy is documented, covering the classification, labelling, and disposition of documents. Organisation has identified and documented Communication in the ISMS Clause Requirements, v2.0	defined and active. Internal and external communications are controlled.
7.5.	Documented information	Information classification policy and document control policy are documented, covering classification, labelling, and disposition of documents. Organisation has identified and Documented Information in the ISMS Clause Requirements, v2.0.	Documented information is well-controlled. Version control and access permissions are implemented and effective.
8.1.	Operational planning and control	Organisation has documented its ISMS plan of action under the ISMS Calendar and identified Operational Planning and Control in the ISMS Clause Requirements, v2.0.	Operations are managed as per documented controls. Implementation is monitored through ISMS calendar activities.
8.2.	Information security risk assessment (ISMS)	The risk assessment methodology is documented. Risk assessment and treatment are documented. Risk ownership is assigned. Risk treatment and acceptance criteria are defined. Organisation has identified and documented it in the ISMS Clause Requirements, v2.0.	Risk assessments are performed periodically. Sample assessments demonstrate effectiveness of risk identification and analysis.
8.3.	Information security risk treatment (ISMS)	The risk assessment methodology is documented. Risk assessment and treatment are documented. Risk ownership is assigned. Risk treatment and acceptance criteria are defined. Organisation has identified and documented it in the ISMS Clause Requirements, v2.0.	Risk treatment plans are implemented. Status and residual risk are documented. Controls are mapped to the SoA.
9.1.	Monitoring,	ISMS functional level objectives	Monitoring metrics and dashboards

	measurement, analysis and evaluation	are measured. Organisation has identified and documented it in the ISMS Clause Requirements, v2.0.	are implemented. Trends and anomalies are reviewed in management reviews.
9.2.	Internal audit (Mentioned) Internal Plan: Internal Date: No. of Internal Auditors: Area's and Department Covered: Total NC's and Observation: Current Closure Status: Verification of Corrective Action: Effectiveness of Internal Audit /Corrective Action: Next Internal Audit Plan: and Frequency:	Internal audit process is documented. Audits are conducted bi-annually as per the documented process. The annual calendar is maintained. The audit is conducted by an external consultant. Findings are tracked in a CAPA tracker. RCA and corrective actions are documented. The topics are covered as per clause 9.2 and Organisation has documented in the ISMS Clause Requirements, v2.0.	The internal audit is conducted at least annually and last audit was conducted by an external consultant on December 16, 2025, during which 7 findings were reported. All findings have since been closed. The findings are tracked in a CAPA tracker, with root cause analyses (RCA) and corrective actions documented. Effective tracking and resolution were observed.
9.3.	Management review-Mentioned MRM Notice: MRM Agenda: MRM Date: Participants: Decision: Continual Improvement: Responsibility:	Records related to ISMS review are documented and stored in the ISMS repository. Management Review Meeting Procedure defines the process for the Management Review of ISMS. Has covered topics as per clause 9.3 and Organisation has documented in the ISMS Clause Requirements, v2.0.	Management review was done on December 17, 2025. MRM minutes verified. All agenda items addressed. Action items from the review have been assigned and are in progress.

	Timeline to Complete Decision/Continual Improvement Plan: Next MRM Due Date and Frequency:		
10	Improvement	Process for Improvement is defined and Organisation has documented in ISMS Clause Requirements, v2.0. The information security incident process is documented covering incident identification, reporting, classification, and resolution. Three security incidents are reported. The incidents are logged in an incident record. The BCP process is documented and the BCP calendar is available.	Incident handling was effective. Lessons learned and preventive actions documented. BCP tests completed as per calendar. No major gaps noted. The production, development and testing environment infrastructure is hosted in the AWS cloud.
	ANNEXURE (For SOA Controls)		
A.5.1	Policies for information security	Organisation has identified and documented it in the Information Security Policy document, v1.0	Various ISMS policies are defined, approved by management, and communicated to and acknowledged by employees. The policies are reviewed annually.
A.5.2	Information security roles and responsibilities	Organisation has identified and documented it in Information Security Roles and Responsibilities, v1.0, in the Information Security Policy, v1.0	Roles and responsibilities are defined and reviewed & approved by top management annually.
A.5.3	Segregation of duties	Organisation has identified and documented it in Information Security Roles and Responsibilities, v1.0, and in	The list of employees document defines all employees' functions, designations, and job descriptions.

		Information Security Policy, v1.0	
A.5.4	Management responsibilities	Organisation has identified and documented it in the Information Security Policy, v1.0, and HR Security Policy, v2.0	Management responsibilities are defined and communicated. The policies are reviewed annually.
A.5.5	Contact with authorities	Organisation has identified and documented it in ISMS Clause Requirements, v1.0	The organization maintains contact with relevant authorities according to the communication procedure. The policy is reviewed annually
A.5.6	Contact with special interest groups	Organisation has identified and documented it in ISMS Clause Requirements, v2.0	The organization maintains contact with special interest groups or other specialist security forums and professional associations.
A.5.7	Threat intelligence	Organisation has identified and documented it in Threat Intelligence Policy, v2.0	Information relating to information security threats is collected and analysed to produce threat intelligence.
A.5.8	Information security in project management	Organisation has identified and documented it in the Information Security Policy, v1.0, and in the Business Continuity and Disaster Recovery Policy, v2.0	The organization has integrated Information security into project management.
A.5.9	Inventory of information and other associated assets	Organisation has identified and documented it in Asset Management and Media Handling Procedure, v2.0	An inventory of information and other associated assets, including owners, is in place and maintained.
A.5.10	Acceptable use of information and other associated assets	Organisation has identified and documented it in the Acceptable Usage Policy, v2.0	Rules for the acceptable use and procedures for handling information and other associated assets are identified, documented, and implemented.
A.5.11	Return of assets	Organisation has identified and documented it in Asset Management and Media Handling Procedure, v2.0	Personnel and other interested parties return all the organization's assets in their possession upon change or termination of their employment, contract, or agreement.

A.5.12	Classification of information	Organisation has identified and documented it in the Information Classification Policy, v2.0	Information is classified according to the information security needs of the organization based on confidentiality, integrity, availability, and relevant interested party requirements.
A.5.13	Labelling of information	Organisation has identified and documented it in the Information Classification Policy, v2.0	An appropriate set of procedures for information labelling is developed and implemented in accordance with the information classification scheme adopted by the organization.
A.5.14	Information transfer	Organisation has identified and documented it in Network Management Policy, v1.0	Information transfer rules, procedures, or agreements are in place for all types of transfer facilities within the organization and between the organization and other parties.
A.5.15	Access control	Organisation has identified and documented it in the Access Control Policy, v2.0	Rules to control physical and logical access to information and other associated assets are established and implemented based on business and information security requirements.
A.5.16	Identity management	Organisation has identified and documented it in the Access Control Policy, v2.0	The full life cycle of identities is managed.
A.5.17	Authentication information	Organisation has identified and documented it in Access Control Policy, v2.0, and Password Management Policy, v1.0, and ISMS Roles and Responsibilities, v1.0	Allocation and management of authentication information is controlled by a management process, including advising personnel on the appropriate handling of authentication information. Multi-factor authentication enforced across critical systems such as AWS IAM, Bitbucket Code Repository etc.
A.5.18	Access rights	Organisation has identified and documented it in the Access	Access rights to information and other associated assets are

		Control Policy, v2.0	provisioned, reviewed, modified, and removed in accordance with the organization's topic-specific policy and rules for access control. Verified the IAM settings to determine that several groups have been formed for different teams and only the production group has access to production resources. Opportunity for Improvement - Access revocation completion date can be documented for better tracking.
A.5.19	Information security in supplier relationships	Organisation has identified and documented it in Vendor Management Policy, v1.0	Processes and procedures are defined and implemented to manage the information security risks associated with the use of the supplier's products or services.
A.5.20	Addressing information security within supplier agreements	Organisation has identified and documented it in Vendor Management Policy, v1.0	Relevant information security Requirements are established and agreed upon with each supplier based on the type of supplier relationship.
A.5.21	Managing information security in the information and communication technology (ICT) supply chain	Organisation has identified and documented it in Vendor Management Policy, v1.0	Processes and procedures are defined and implemented to manage the information security risks associated with the ICT products and services supply chain.
A.5.22	Monitoring, review and change management of supplier services	Organisation has identified and documented it in Vendor Management Policy, v1.0	The organization regularly monitors, reviews, evaluates, and manages changes in supplier information security practices and service delivery.
A.5.23	Information security for use of cloud services	Organisation has identified and documented it in Cloud Security Policy, v1.0	Processes for acquisition, use, management and exit from the cloud services are established in accordance with the organization's

			information security requirements. AWS security configurations is regularly reviewed and updated.
A.5.24	Information security incident management planning and preparation	Organisation has identified and documented it in Incident Management Policy, v1.0	The organization plans and prepares managing information security incidents by defining, establishing, and communicating information security incident management processes, roles and responsibilities.
A.5.25	Assessment and decision on information security events	Organisation has identified and documented it in Incident Management Policy, v1.0	The organization assesses information security events and decides if they are to be categorized as information security incidents.
A.5.26	Response to information security incidents	Organisation has identified and documented it in Incident Management Policy, v1.0	Information security incidents are responded to in accordance with the documented procedures.
A.5.27	Learning from information security incidents	Organisation has identified and documented it in Incident Management Policy, v1.0	Knowledge gained from information security incidents are used to strengthen and improve the information security controls.
A.5.28	Collection of evidence	Organisation has identified and documented it in Incident Management Policy, v1.0	The organization establishes and implements procedures for the identification, collection, acquisition and preservation of evidence related to information security events.
A.5.29	Information security during disruption	Organisation has identified and documented it in Business Continuity and Disaster Recovery Policy, v2.0	The organization has planned how to maintain information security at an appropriate level during disruption.
A.5.30	ICT readiness for business continuity	Organisation has identified and documented it in Business Continuity and Disaster Recovery Policy, v2.0	ICT readiness has been planned, implemented, maintained, and tested based on business continuity objectives and ICT continuity requirements. Verified the BCP DR drill report dated December 06, 2025 and noted that test was conducted.

A.5.31	Legal, statutory, regulatory and contractual requirements	Organisation has identified and documented it in Encryption and Key Management Policy, v2.0	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements is identified, documented, and kept up to date.
A.5.32	Intellectual property rights	Organisation has identified and documented it in Information Classification Policy, v2.0and Asset Management and Media Handling Procedure, v2.0	The organization has implemented appropriate procedures to protect intellectual property rights.
A.5.33	Protection of records	Organisation has identified and documented it in Data Privacy Policy, v2.0, and in Data and Record Retention and Deletion Policy, v2.0	Records are protected from loss, destruction, falsification, unauthorized access, and unauthorized release.
A.5.34	Privacy and protection of personal identifiable information (PII)	Organisation has identified and documented it in Mobile Device and Teleworking Policy, v2.0, and Data Privacy Policy, v2.0	The organization has identified and met the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.
A.5.35	Independent review of information security	Organisation has identified and documented it in Information Security Policy, v1.0, and Internal Audit, Continual Improvement And Non - Conformity and Corrective Action Policy, v2.0	The organization's approach to managing information security and its implementation including people, processes and technologies are reviewed independently at the planned intervals, or when significant changes occur.
A.5.36	Compliance with policies, rules and standards for information security	Organisation has identified and documented it in Management Review Meeting Procedure, v1.0, Internal Audit, Continual Improvement And Non - Conformity and Corrective Action Policy, v2.0, and Document Control Procedure, v2.0	Compliance with the organization's information security policy, topic-specific policies, rules and standards are regularly reviewed.
A.5.37	Documented	Operating procedures for	Operating procedures for

	operating procedures	information security are documented and updated regularly.	information processing facilities is documented and made available to personnel who need them.
A.6.1	Screening	Organisation has identified and documented it in HR Security Policy, v2.0	Background verification checks on all candidates to become personnel is carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations, and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. Verified that sampled employee Rxxxxxh joined on May 30, 2025 screening was done with relevant laws and rules.
A.6.2	Terms and conditions of employment	The employment contractual agreements state the personnel's and the organization's responsibilities for information security.	The employment contractual agreements state the personnel's and the organization's responsibilities for information security. Verified that for sampled candidate Rxxxxxh joined on May 30, 2025, employee agreement and NDA was signed in accordance with relevant laws and regulations.
A.6.3	Information security awareness, education and training	Personnel of the organization and relevant interested parties receive appropriate information security awareness, education and training and regular updates on the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	Personnel of the organization and relevant interested parties receive appropriate information security awareness, education and training and regular updates on the organization's information security policy, topic-specific policies and procedures, as relevant for their job function. Verified that sampled candidate Rxxxxxh joined on May 30, 2025 has completed ISMS training.
A.6.4	Disciplinary process	Organisation has identified and documented it in HR Disciplinary	A disciplinary process is formalized and communicated to take actions

		Policy & Procedure, v2.0	against personnel and other relevant interested parties who have committed an information security policy violation. Verified that sampled candidate Rxxxxxh joined on May 30, 2025 has signed code of conduct.
A.6.5	Responsibilities after termination or change of employment	Organisation has identified and documented it in HR Disciplinary Policy & Procedure, v2.0, and in Information Security Policy, v1.0	Information security responsibilities and duties that remain valid after termination or change of employment is defined, enforced and communicated to relevant personnel and other interested parties. Verified that sampled candidate Rxxxxxh Sxxxxxxxxv left the organization on July 24, 2025 and respective accounts access were taken in accordance with relevant laws and regulations.
A.6.6	Confidentiality or non-disclosure agreements	Organisation has identified and documented it in HR Disciplinary Policy & Procedure, v2.0	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information is identified, documented, regularly reviewed and signed by personnel and other relevant interested parties. Verified that for sampled candidate Rxxxxxh joined on May 30, 2025, employee agreement and NDA was signed in accordance with relevant laws and regulations.
A.6.7	Remote working	Organisation has identified and documented it in Mobile Device and Teleworking Policy, v2.0	Security measures are implemented when personnel are working remotely to protect information accessed, processed, or stored outside the organization's premises.
A.6.8	Information security event reporting	Organisation has identified and documented it in Incident Management Policy, v1.0	The organization provides the mechanism for personnel to report observed or suspected information security events through appropriate

			channels in a timely manner.
A.7.1	Physical security perimeters	Not Applicable - As physical security is out of scope for the organisation.	Not Applicable - As physical security is out of scope for the organisation.
A.7.2	Physical entry	Not Applicable - As physical security is out of scope for the organisation.	Not Applicable - As physical security is out of scope for the organisation.
A.7.3	Securing offices, rooms and facilities	Not Applicable - As physical security is out of scope for the organisation.	Not Applicable - As physical security is out of scope for the organisation.
A.7.4	Physical security monitoring	Not Applicable - As physical security is out of scope for the organisation.	Not Applicable - As physical security is out of scope for the organisation.
A.7.5	Protecting against physical and environmental threats	Not Applicable - As physical security is out of scope for the organisation.	Not Applicable - As physical security is out of scope for the organisation.
A.7.6	Working in secure areas	Not Applicable - As physical security is out of scope for the organisation.	Not Applicable - As physical security is out of scope for the organisation.
A.7.7	Clear desk and clear screen	Not Applicable - As physical security is out of scope for the organisation.	Not Applicable - As physical security is out of scope for the organisation.
A.7.8	Equipment siting and protection	Not Applicable - As physical security is out of scope for the organisation.	Not Applicable - As physical security is out of scope for the organisation.
A.7.9	Security of assets off-premises	Not Applicable - As physical security is out of scope for the organisation.	Not Applicable - As physical security is out of scope for the organisation.
A.7.10	Storage media	Not Applicable - As physical security is out of scope for the organisation.	Not Applicable - As physical security is out of scope for the organisation.
A.7.11	Supporting utilities	Not Applicable - As physical security is out of scope for the organisation.	Not Applicable - As physical security is out of scope for the organisation.

A.7.12	Cabling security	Not Applicable - As physical security is out of scope for the organisation.	Not Applicable - As physical security is out of scope for the organisation.
A.7.13	Equipment maintenance	Not Applicable - As physical security is out of scope for the organisation.	Not Applicable - As physical security is out of scope for the organisation.
A.7.14	Secure disposal or re-use of equipment	Not Applicable - As physical security is out of scope for the organisation.	Not Applicable - As physical security is out of scope for the organisation.
A.8.1	User end point devices	Organisation has identified and documented it in Access Control Policy, v2.0, and Asset Management and Media Handling Procedure Policy, v2.0	Information stored on, processed by, or accessible via user end-point devices is protected. Verified that Centralized enforcement for USB blocking and monitoring has been implemented to strengthen USB port control. Opportunity for Improvement - MDM tool can be considered for control of Endpoint devices.
A.8.2	Privileged access rights	Organisation has identified and documented it in Access Control Policy, v2.0	The allocation and use of privileged access rights are restricted and managed.
A.8.3	Information access restriction	Organisation has identified and documented it in Access Control Policy, v2.0	Access to information and other associated assets is restricted in accordance with the established topic-specific policy on access control.
A.8.4	Access to source code	Organisation has identified and documented it in Access Control Policy, v2.0	Read and write access to source code, development tools, and software libraries are appropriately managed. Verified that mechanisms exist to limit privileges to change software resident within software libraries in Bitbucket code repository.
A.8.5	Secure authentication	Organisation has identified and documented it in Access Control Policy, v2.0, and Password	Secure authentication technologies and procedures are implemented based on information access

		Management Policy, v1.0	restrictions and the topic-specific policy on access control.
A.8.6	Capacity management	Organisation has identified and documented it in Information Security (IS) Policy, v2.0	The use of resources is monitored and adjusted in line with current and expected capacity requirements. Verified that AWS CloudWatch has been configured for capacity monitoring and alerts are being generated.
A.8.7	Protection against malware	Organisation has identified and documented it in Antivirus Policy, v2.0	Protection against malware is implemented and supported by appropriate user awareness. Verified antivirus is installed in all the laptops.
A.8.8	Management of technical vulnerabilities	Organisation has identified and documented it in Patch & Vulnerability Management Policy, v1.0	Information about technical vulnerabilities of information systems in use is obtained, the organization's exposure to such vulnerabilities is evaluated and appropriate measures shall be taken. Verified with the latest vulnerability assessment /penetration test report performed on December 04, 2025 and determined that VA/PT are carried out periodically and that vulnerabilities were closed.
A.8.9	Configuration management	Organisation has identified and documented it in Configuration Management Policy, v2.0	Configurations, including security configurations, of hardware, software, services, and networks are established, documented, implemented, monitored, and reviewed.
A.8.10	Information deletion	Organisation has identified and documented it in Mobile Device and Teleworking Policy, v1.0, and Asset Management and Media Handling Procedure, v1.0	Information stored in information systems, devices, or in any other storage media is deleted when no longer required.

A.8.11	Data masking	Organisation has identified and documented it in Encryption and Key Management Policy, v2.0, and Data Retention and Deletion Policy, v2.0	Data masking is used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.
A.8.12	Data leakage prevention	Data leakage prevention measures are applied to systems, networks, and any other devices that process, store, or transmit sensitive information.	Data leakage prevention measures are applied to systems, networks, and any other devices that process, store, or transmit sensitive information.
A.8.13	Information backup	Organisation has identified and documented it in Backup & Restore Policy, v3.0	Backup copies of information, software, and systems are maintained and regularly tested in accordance with the agreed topic-specific policy on backup.
A.8.14	Redundancy of information processing facilities	Organisation has identified and documented it in Business Continuity and Disaster Recovery Policy, v2.0	Information processing facilities are implemented with redundancy sufficient to meet availability requirements.
A.8.15	Logging	Organisation has identified and documented it in Log Management and Monitoring Policy, v2.0	Logs that record activities, exceptions, faults, and other relevant events are produced, stored, protected, and analysed.
A.8.16	Monitoring activities	Organisation has identified and documented it in Log Management and Monitoring Policy, v2.0	Networks, systems, and applications are monitored for anomalous behavior, and appropriate actions are taken to evaluate potential information security incidents.
A.8.17	Clock synchronization	Organisation has identified and documented it in System, IT Hardening Guidelines, v2.0	The clocks of information processing systems used by the organization are synchronized to approved time sources.
A.8.18	Use of privileged utility programs	Organisation has identified and documented it in Access Control Policy, v2.0	The use of utility programs that can be capable of overriding system and application controls are restricted

			and tightly controlled.
A.8.19	Installation of software on operational systems	Not Applicable	Not Applicable
A.8.20	Networks security	Organisation has identified and documented it in Network Management Policy, v1.0	Networks and network devices are secured, managed, and controlled to protect information in systems and applications. Verified that AWS Security Groups has been setup for Managing incoming and outgoing connection settings.
A.8.21	Security of network services	Organisation has identified and documented it in Network Management Policy, v1.0	Security mechanisms, service levels, and service requirements of network services are identified, implemented, and monitored.
A.8.22	Segregation of networks	Organisation has identified and documented it in Network Management Policy, v1.0	Groups of information services, users, and information systems are segregated in the organization's networks.
A.8.23	Web filtering	Organisation has identified and documented it in Antivirus Policy, v2.0	Access to external websites is managed to reduce exposure to malicious content.
A.8.24	Use of cryptography	Organisation has identified and documented it in Encryption and Key Management Policy, v2.0	Rules for the effective use of cryptography, including cryptographic key management, are defined and implemented. Verified SSH settings in SSH client to determine that encrypted SSH key is required for connecting to AWS Cloud infrastructure.
A.8.25	Secure development life cycle	Organisation has identified and documented it in Change Management Policy & Procedure, v2.0and Secure Development and Maintenance Policy, v2.0	Rules for the secure development of software and systems shall be established and applied.

A.8.26	Application security requirements	Organisation has identified and documented it in Encryption and Key Management Policy, v2.0	Information security requirements are identified, specified, and approved when developing or acquiring applications.
A.8.27	Secure system architecture and engineering principles	Organisation has identified and documented it in Access Control Policy, v2.0 and Secure Development and Maintenance Policy, v2.0	Principles for engineering secure systems are established, documented, maintained, and applied to any information system development activities.
A.8.28	Secure coding	Organisation has identified and documented it in Secure Development and Maintenance Policy, v2.0	Secure coding principles are applied to software development. Verified with code review results of Bitbucket code repository.
A.8.29	Security testing in development and acceptance	Organisation has identified and documented it in Secure Development and Maintenance Policy, v2.0	Security testing processes are defined and implemented in the development life cycle.
A.8.30	Outsourced development	All the developments are done in-house and no outsourcing required. Therefore, the Outsourced System Development is not in scope	NA - All the developments are done in-house and no outsourcing required. Therefore, the Outsourced System Development is not in scope.
A.8.31	Separation of development, test and production environments	Organisation has identified and documented it in Secure Development and Maintenance Policy, v2.0	Development, testing, and production environments are separated and secured.
A.8.32	Change management	Organisation has identified and documented it in Change Management Policy & Procedure, v2.0	Changes to information processing facilities and information systems are subject to change management procedures.
A.8.33	Test information	Organisation has identified and documented it in Secure Development and Maintenance Policy, v2.0	Test information is appropriately selected, protected, and managed.
A.8.34	Protection of information systems during audit testing	Organisation has identified and documented it in Log Management and Monitoring Policy, v2.0 , and Internal Audit,	Audit tests and other assurance activities involving the assessment of operational systems are planned and agreed upon between the tester

		Continual Improvement And Non - Conformity and Corrective Action Policy, v2.0	and appropriate management.