STATEMENT OF APPLICABILITY

ISO 27001:2013 Annex A – Control Objectives and Controls

ISO 27001 Clause No	Control	Applicable (Yes/No)	Justification	Reference Document
A.5 INFORMATION SECURITY POLICIES				
A.5.1 Management direction for information security				
A.5.1.1	Policies for information security	Yes	To provide management direction.	ISMS Policies
A.5.1.2	Review of policies for Information Security	Yes	This is baseline control needed to review the changes to policy in light of business needs and technology changes	Procedure for Document Control, Record of Management Review Meeting
A.6 ORGANIZATION OF INFORMATION SECURITY				
A.6.1 Internal organization				
A.6.1.1	Information security roles and responsibilities	Yes	Baseline control so that everyone understands about their responsibilities.	ISMS Manual – Roles and Responsibilities
A.6.1.2	Segregation of duties	Yes	Required to ensure everyone is aware of their responsibilities and there are no conflicts	Roles and Responsibilities defined in ISMS Manual

ISO 27001 Clause No	Control	Applicable (Yes/No)	Justification	Reference Document
A.6.1.3	Contact with authorities	Yes	Baseline control to ensure proper implementation of ISMS .	List of contact details like ISP's, government agencies etc.
A.6.1.4	Contact with special interest groups	Yes	Required after assessing the Risks involved.	Memberships with various security forums – IT Administrator
A.6.1.5	Information security in project management	Yes	Required to ensure that every project addresses information security.	Procedure of security in project management.
A.6.2 Mobile devices and Tele-working				
A.6.2.1	Mobile device policy	No	No Mobile computing done	
A.6.2.2	Tele-working	No	No tele-working done	
A.7 HUMAN RESOURCES SECURITY				
A.7.1 Prior to employment				
A.7.1.1	Screening	Yes	Required to reduce risk of human errors.	ISMS/POL/003 Human Resources Policy

ISO 27001 Clause No	Control	Applicable (Yes/No)	Justification	Reference Document
A.7.1.2	Terms and conditions of employment	Yes	Baseline control to ensure proper implementation of ISMS.	ISMS/POL/003 Human Resources Policy Terms and Conditions provided to Employees during recruitment.
A.7.2 During employment				
A.7.2.1	Management responsibilities	Yes	Baseline control so that everyone understands about their responsibilities.	Roles and Responsibilities defined in ISMS Manual
A.7.2.2	Information security awareness, education and training	Yes	To train the users about ISMS.	Training Calendar, Training material
A.7.2.3	Disciplinary process	No	Not required	Disciplinary action is not required.
A.7.3 Termination or change of employment				
A.7.3.1	Termination or change of employment responsibilities.	Yes	Baseline control needed to address security risks when an employee leaves.	Termination Checklist. ISMS/POL/003 Human Resources Policy

ISO 27001 Clause No	Control	Applicable (Yes/No)	Justification	Reference Document
A.8 ASSET MANAGEMENT				
A.8.1 Responsibility for assets				
A.8.1.1	Inventory of Assets	Yes	Baseline control to ensure that proper list of assets is maintained.	List of Assets
A.8.1.2	Ownership of assets	Yes	Baseline control to ensure that proper list of assets is maintained.	List of Assets
A.8.1.3	Acceptable use of assets	Yes	Baseline control to ensure that proper list of assets is maintained.	ISMS/POL/002 Acceptable Usage Policy
A.8.1.4	Return of assets	Yes	Baseline control needed to address security risks when an employee leaves.	ISMS/POL/003 Human Resources Policy
A.8.2 Information classification				
A.8.2.1	Classification of information	Yes	Baseline control to ensure proper implementation of ISMS.	ISMS/P/01 - Risk Assessment Procedure
A.8.2.2	Labelling of information	Yes	Baseline control to ensure proper implementation of ISMS.	ISMS/P/01 - Risk Assessment Procedure

ISO 27001 Clause No	Control	Applicable (Yes/No)	Justification	Reference Document
A.8.2.3	Handling of assets	Yes	Required for security of removable media.	ISMS/P-10 Information Handling and Exchange Procedure
A.8.3 Media handling				
A.8.3.1	Management of removable media	Yes	Required for security of removable media.	ISMS/POL/008 – Media Handling Policy
A.8.3.2	Disposal of media	Yes	Required for security of removable media during disposal.	ISMS/POL/008 – Media Handling Policy
A.8.3.3	Physical media transfer	Yes	Required to protect the media in transit	ISMS/POL/008 – Media Handling Policy
A.9 ACCESS CONTROL				
A.9.1 Business Requirements of Access Control				
A.9.1.1	Access control policy	Yes	Required to control access to information.	ISMS/POL/011 Access Control Policy and Procedure
A.9.1.2	Policy on use of network services	Yes	Required for security of the networks.	ISMS/POL/007 – Network Security Policy and Procedure
A.9.2 User Access Management				
A.9.2.1	User registration and deregistration	Yes	Required to grant user access to information systems.	ISMS/POL/011 Access Control Policy and Procedure Records of Users Registered.

ISO 27001 Clause No	Control	Applicable (Yes/No)	Justification	Reference Document
A.9.2.2	User access provisioning	Yes	Required for monitoring purpose.	ISMS/POL/012 – Operating System Security Policy and Procedure
A.9.2.3	Management of privilege access rights	Yes	Required to monitor and review privileges given.	ISMS/POL/011 Access Control Policy and Procedure
A.9.2.4	Management of secret authentication information of users	Yes	Required for allocation of passwords to the user.	ISMS/POL/012 Password Management Policy and Procedure
A.9.2.5	Review of user access rights	Yes	Required for reviewing of access rights allocated.	ISMS/POL/011 Access Control Policy and Procedure
A.9.2.6	Removal or adjustment of access rights	Yes	Baseline control needed to address security risks when an employee leaves.	ISMS/POL/003 Human Resources Policy
A.9.3 User Responsibilities				
A.9.3.1	Use of secret authentication information	Yes	Required to follow good practices with password usage.	ISMS/POL/012 Password Management Policy and Procedure
A.9.4 System and Application Access Control				
A.9.4.1	Information access restriction	Yes	Required after assessing the Risks involved.	ISMS/POL/011 Access Control Policy and Procedure

ISO 27001 Clause No	Control	Applicable (Yes/No)	Justification	Reference Document
A.9.4.2	Secure log-on procedures	Yes	Required for security of information processing systems from unauthorized login/access.	ISMS/POL/012 – Operating System Security Policy and Procedure
A.9.4.3	Password management system	Yes	Required to manage passwords.	ISMS/POL/012 Password Management Policy and Procedure
A.9.4.4	Use of privileged utility programs	Yes	Required to control the misuse of system utilities	ISMS/POL/011 Access Control Policy and Procedure
A.9.4.5	Access control to program source code	Yes	Required to protect the source code from unauthorized access and modification.	ISMS/P-07/ Software Development and Testing Procedure Access control logs
A.10 CRYPTOGRAPHY				
A.10.1 Cryptographic Controls				
A.10.1.1	Policy on the use of cryptographic controls	No	Company does not use cryptographic controls.	
A.10.1.2	Key management	No	Company does not use cryptographic controls.	

ISO 27001 Clause No	Control	Applicable (Yes/No)	Justification	Reference Document
A.11 PHYSICAL AND ENVIRONMENTAL SECURITY				
A.11.1 Secure Areas				
A.11.1.1	Physical security perimeter	Yes	Required after assessing the Risks involved to protect the business premise.	ISMS/P-04 - Procedure on Physical and Environment security
A.11.1.2	Physical entry controls	Yes	Required after assessing the Risks involved to protect the business premise.	ISMS/P-04 - Procedure on Physical and Environment security Physical Entry Records
A.11.1.3	Securing offices, rooms and facilities	Yes	Required after assessing the Risks involved to protect the business premise.	ISMS/P-04 - Procedure on Physical and Environment security
A.11.1.4	Protecting against external and environmental threats	Yes	Required after assessing the Risks involved to protect against environment threats.	ISMS/P-04 - Procedure on Physical and Environment security
A.11.1.5	Working in secure areas	Yes	Required after assessing the Risks involved.	ISMS/P-04 - Procedure on Physical and Environment security

ISO 27001 Clause No	Control	Applicable (Yes/No)	Justification	Reference Document
A.11.1.6	Delivery and loading areas	No	No delivery and loading areas.	
A.11.2 Equipment				
A.11.2.1	Equipment siting and protection	Yes	Required for equipment security after assessing the Risks involved.	ISMS/P-04 - Procedure on Physical and Environment security
A.11.2.2	Supporting Utilities	Yes	Required for equipment security after assessing the Risks involved.	ISMS/P-04 - Procedure on Physical and Environment security
A.11.2.3	Cabling Security	Yes	Required for equipment security after assessing the Risks involved.	ISMS/P-04 - Procedure on Physical and Environment security Cabling and Network Diagram
A.11.2.4	Equipment maintenance	Yes	Required for equipment security after assessing the Risks involved.	ISMS/POL-05 Equipment Maintenance Policy Equipment Maintenance Records

ISO 27001 Clause No	Control	Applicable (Yes/No)	Justification	Reference Document
A.11.2.5	Removal of assets	Yes	Required for equipment security after assessing the Risks involved.	ISMS/POL-06/Equipment Disposal and Removal Policy Removal Records
A.11.2.6	Security of equipment off-premises	Yes	Required for equipment security after assessing the Risks involved.	ISMS/P-04 - Procedure on Physical and Environment security
A.11.2.7	Secure disposal or re-use of equipment	Yes	Required for equipment security after assessing the Risks involved.	ISMS/POL-06/Equipment Disposal and Removal Policy Disposal Records
A.11.2.8	Unattended user equipment	Yes	Required for protection of user equipments.	ISMS/P-10 Information Handling and Exchange Procedure
A.11.2.9	Clear desk and clear screen policy	Yes	Required for protection of user equipments.	ISMS/P-10 Information Handling and Exchange Procedure

ISO 27001 Clause No	Control	Applicable (Yes/No)	Justification	Reference Document
A.12 OPERATIONS SECURITY				
A.12.1 Operational Procedures and Responsibilities				
A.12.1.1	Documented operating procedures	Yes	Required for correct and secure operation of information processing facilities.	ISMS/P-05/ Documented Operating Procedure
A.12.1.2	Change Management	Yes	Required to manage all changes	ISMS/P-06/ Change Management Procedure Change Management Records
A.12.1.3	Capacity management	Yes	To ensure that the information processing facility has enough capacity to meet business requirements.	ISMS/P-09/ Capacity Management Procedure
A.12.1.4	Separation of development, testing and operational environments.	Yes	To protect the production environment.	ISMS/P-07/ Software Development and Testing Procedure
A.12.2 Protection from Malware				
A.12.2.1	Control against malware	Yes	To protect from virus threats.	ISMS/POL/005 - Protection from Malicious Code Policy

ISO 27001 Clause No	Control	Applicable (Yes/No)	Justification	Reference Document
A.12.3 Back-up				
A.12.3.1	Information backup	Yes	To maintain the integrity and availability of data	ISMS/POL/006 – Backup Policy Backup Records. Records of Testing
A.12.4 Logging and Monitoring				
A.12.4.1	Event logging	Yes	Required to monitor use of business information systems.	ISMS/POL/010 Logging and Monitoring Policy
A.12.4.2	Protection of log information	Yes	Required to monitor use of business information systems.	ISMS/POL/010 Logging and Monitoring Policy
A.12.4.3	Administrator and operator logs	Yes	Required to monitor use of business information systems.	ISMS/POL/010 Logging and Monitoring Policy
A.12.4.4	Clock synchronization	No	Not required for business process	
A.12.5 Control of Operational Software				
A.12.5.1	Installation of software on operational systems	Yes	Required after assessing the Risks involved.	ISMS/P-07/ Software Development and Testing Procedure Logs of all updates

ISO 27001 Clause No	Control	Applicable (Yes/No)	Justification	Reference Document
A.12.6 Technical Vulnerability Management				
A.12.6.1	Control of technical vulnerabilities	Yes	To fix all vulnerabilities.	ISMS/POL/012 – Operating System Security Policy and Procedure
A.12.6.2	Restrictions on software installations	Yes	This control is required to ensure that unauthorized software is not installed on machines which may create vulnerabilities in the system.	ISMS/POL/012 – Operating System Security Policy and Procedure
A.12.7 Information System Audit Considerations				
A.12.7.1	Information systems audit controls	Yes	Baseline control to ensure the compliance with ISO 27001	ISMS/P-02 Internal Audit Procedure Internal Audit Records
A.13 COMMUNICATIONS SECURITY				
A.13.1 Network Security Management				
A.13.1.1	Network controls	Yes	Required for security of the networks.	ISMS/POL/007 – Network Security Policy

ISO 27001 Clause No	Control	Applicable (Yes/No)	Justification	Reference Document
A.13.1.2	Security of network services	Yes	Required for security of the networks.	ISMS/POL/007 – Network Security Policy
A.13.1.3	Segregation in networks	Yes	Required for security of the networks.	ISMS/POL/007 – Network Security Policy and Procedure
A.13.2 Information Transfer				
A.13.2.1	Information transfer policies and procedures	Yes	This control is required to cover the information exchange.	ISMS/P-10 Information Handling and Exchange Procedure
A.13.2.2	Agreements on information transfer	Yes	This control is required to cover the information exchange.	Exchange Agreements
A.13.2.3	Electronic messaging	Yes	Required considering the risks involved	ISMS/POL/009 – Email Policy
A.13.2.4	Confidentiality or non-disclosure	Yes	Baseline control to ensure proper implementation of ISMS.	Records of Terms and conditions of employment and NDA's signed with employees.

ISO 27001 Clause No	Control	Applicable (Yes/No)	Justification	Reference Document
A.14 SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE				
A.14.1 Security requirements of information systems				
A.14.1.1	Information security requirements analysis and specifications	Yes	To ensure security features are identified and built into the application.	ISMS/P-07/ Software Development and Testing Procedure
A.14.1.2	Securing application services on public networks	Yes	Required considering the risks involved with ecommerce activities.	ISMS/P-11 E-commerce Security Procedure
A.14.1.3	Protecting application services transactions	Yes	Required considering the risks involved with ecommerce activities.	ISMS/P-11 E-commerce Security Procedure
A.14.2 Security in Development and Support Processes				
A.14.2.1	Secure development policy	Yes	To ensure security features during development	ISMS/POL-14/ Secure development policy
A.14.2.2	System change control procedures	Yes	To monitor and control changes in the software.	ISMS/P-06/ Change Management Procedure Change Management Records

ISO 27001 Clause No	Control	Applicable (Yes/No)	Justification	Reference Document
A.14.2.3	Technical review of applications after operating platform changes	Yes	To protect the application after any changes in OS.	ISMS/P-07/ Software Development and Testing Procedure
A.14.2.4	Restrictions on changes to software packages	No	Vendor supplied packages are not changed by the company	
A.14.2.5	Secure system engineering principles	Yes	To ensure that best practices are followed	ISMS/POL-14/ Secure development policy
A.14.2.6	Secure development environment	Yes	To protect the development environment from unauthorized changes	ISMS/POL-14/ Secure development policy
A.14.2.7	Outsourced development	No	The Organization does not outsource its software development.	
A.14.2.8	System security testing	Yes	To ensure that adequate security is addressed in the system.	ISMS/P-07/ Software Development and Testing Procedure
A.14.2.9	System acceptance	Yes	To ensure that the systems are as per requirements.	ISMS/POL/001 - Authorization and Acceptance Policy

ISO 27001 Clause No	Control	Applicable (Yes/No)	Justification	Reference Document
A.14.3 Test data				
A.14.3.1	Protection of test data	Yes	No	No test data received from any customers. So not required to protect the same.
A.15 SUPPLIER RELATIONSHIPS				
A.15.1 Information security in supplier relationships				
A.15.1.1	Information security policy for supplier relationships	Yes	To ensure security while dealing with suppliers	ISMS/POL-15 Information security in supplier relationship Policy and Procedure
A.15.1.2	Addressing security within supplier agreements	Yes	Baseline control to ensure proper implementation of ISMS.	Confidentiality agreements and SLA with Suppliers
A.15.1.3	Information and communication technology supply chain	Yes	To ensure security in the supply chain	ISMS/POL-15 Information security in supplier relationship Policy and Procedure
A.15.2 Supplier Service Delivery Management				
A.15.2.1	Monitoring and review of supplier services	Monitoring and review of third party services	Yes	Required to monitor third party service delivery

ISO 27001 Clause No	Control	Applicable (Yes/No)	Justification	Reference Document
A.15.2.2	Managing changes to supplier services	Managing changes to third party services	Yes	Required to monitor third party service delivery
A.16 INFORMATION SECURITY INCIDENT MANAGEMENT				
A.16.1 Management of Information Security Incidents and Improvements				
A.16.1.1	Responsibilities and procedures	Yes	To ensure that users are aware of their responsibilities	ISMS/POL/013 – Incident Management Policy and Procedure
A.16.1.2	Reporting information security events	Yes	Baseline control for incident management	ISMS/POL/013 – Incident Management Policy and Procedure Security Incident Reporting Forms
A.16.1.3	Reporting security weakness	Yes	Baseline control for incident management	ISMS/POL/013 – Incident Management Policy and Procedure Security Incident Reporting Forms
A.16.1.4	Assessment of and decision on information security events	No	All events are logged as information security incidents	

ISO 27001 Clause No	Control	Applicable (Yes/No)	Justification	Reference Document
A.16.1.5	Response to information security incidents	Yes	To ensure that action is taken without any delay	ISMS/POL/013 – Incident Management Policy and Procedure
A.16.1.6	Learning from information security incidents	Yes	To prevent occurrence of the incidents in future.	ISMS/POL/013 – Incident Management Policy and Procedure Incident Register
A.16.1.7	Collection of evidence	Yes	To use them as evidence in court of law.	ISMS/POL/013 – Incident Management Policy and Procedure Incident Register
A.17 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT				
A.17.1 Information Security Continuity				
A.17.1.1	Planning information security continuity	Yes	Baseline control to ensure that the business continues in event of any major failure or disaster.	ISMS/P-13 Business Continuity Plan Business Impact Analysis Report
A.17.1.2	Implementing information security continuity	Yes	Baseline control to ensure that the business continues in event of any major failure or disaster.	ISMS/P-13 Business Continuity Plan

ISO 27001 Clause No	Control	Applicable (Yes/No)	Justification	Reference Document
A.17.1.3	Verify, review and evaluate information security continuity	Yes	To ensure that the restoration is possible when disaster strikes.	ISMS/P-13 Business Continuity Plan
A.17.2 Redundancies				
A.17.2.1	Availability of information processing facilities			
A.18 COMPLIANCE				
A.18.1 Compliance with Legal and Contractual Requirements				
A.18.1.1	Identification of applicable legislation and contractual requirements	Yes	To avoid breaches of any applicable civil and criminal law, statutory, regulatory or contractual obligations.	List of Applicable Laws
A.18.1.2	Intellectual property rights (IPR)	Yes	To ensure that all licensed software are used.	ISMS/POL/013 IPR and Data Protection Policy and Procedure Software Licences Report

ISO 27001 Clause No	Control	Applicable (Yes/No)	Justification	Reference Document
A.18.1.3	Protection of records	Yes	All records maintained as per statutory and regulatory requirements.	ISMS/POL/013 IPR and Data Protection Policy and Procedure
A.18.1.4	Privacy and protection of personally identifiable information	Yes	Required after assessing the Risks involved.	ISMS/POL/013 IPR and Data Protection Policy and Procedure
A.18.1.5	Regulation of cryptographic controls	No	Company does not use cryptographic controls.	
A.18.2 Information Security Reviews				
A.18.2.1	Independent review of information security	Yes	Baseline control required to assess the adequacy, suitability and efficacy of ISMS	Procedure on Internal Audits.
A.18.2.2	Compliance with security policies and standards	Yes	Baseline control to ensure the compliance with ISO 27001	ISMS/P-02 Internal Audit Procedure Internal Audit Records
A.18.2.3	Technical compliance review	Yes	Baseline control to ensure the compliance with ISO 27001	Vulnerability Assessment and Penetration Testing Reports