Demo Company Limited		
Statement of Applicability		
ISO/IEC 27001:2013		
Issue 1	**Clause 6.1.3d**	**Authorised By:- Directors of Demo Company Limited**
Page 1 of 24	**Effective Date: 1st Nov 2021**	**Classification: - Internal**
Issue Date: 1st Nov 2021	**Last Review Date: 1st Nov 2021**	

Annex #	Title	Control Required	Applicable (Y/N)	Controls Applied
A.5	**Information Security Policies**			
A.5.1	Management direction for information security			
Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.				
A.5.1.1	Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	Y	Information Security Procedure
A.5.1.2	Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Y	Information Policy Review Process
A.6	**Organisation of Information Security**			
A.6.1	Internal organisation			
Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organisation.				
A.6.1.1	Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.	Y	Organisation of Information Security
A.6.1.2	Segregation of duties	Conflicting duties and areas of responsibility shall		Organisation of Information Security

		be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.	Y	
A.6.1.3	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	Y	Organisation of Information Security
A.6.1.4	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	Y	Organisation of Information Security
A.6.1.5	Information security in project management	Information security shall be addressed in project management, regardless of the type of project.	Y	Organisation of Information Security
A.6.2	Mobiles devices and teleworking			
Objective: To ensure the security of teleworking and use of mobile devices.				
A.6.2.1	Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	Y	Mobile Device Policy
A.6.2.2	Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	Y	Teleworking Policy
A.7	**Human resource security**			
A.7.1	Prior to employment			
Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.				

A.7.1.1	Screening	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Y	Human Resource Security
A.7.1.2	Terms and conditions of employment	The contractual agreements with employees and contractors shall state their and the organisation's responsibilities for information security.	Y	Human Resource Security
A.7.2	During employment			
Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.				
A.7.2.1	Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation.	Y	Information Security Awareness Program Process
A.7.2.2	Information security awareness, education and training	All employees of the organisation and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organisational policies and	Y	Information Security Awareness Program Process

		procedures, as relevant for their job function.		
A.7.2.3	Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	Y	Information Security Awareness Program Process
A.7.3	Termination and change of employment			
Objective: To protect the organisation's interests as part of the process of changing or terminating employment.				
A.7.3.1	Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	Y	Termination or Change of Employment Controls for Employees & Contractors
A.8	**Asset management**			
A.8.1	Responsibility for assets			
Objective: To identify organisational assets and define appropriate protection responsibilities.				
A.8.1.1	Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	Y	Asset Management

A.8.1.2	Ownership of assets	Assets maintained in the inventory shall be owned.	Y	Asset Management
A.8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	Y	Asset Management
A.8.1.4	Return of assets	All employees and external party users shall return all of the organisational assets in their possession upon termination of their employment, contract or agreement.	Y	Asset Management
A.8.2	Information classification			
Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organisation.				
A.8.2.1	Classification of information	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	Y	Asset Classification Procedure
A.8.2.2	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organisation.	Y	Asset Classification Procedure
A.8.2.3	Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the	Y	Asset Classification Procedure Password Control Procedure

		information classification scheme adopted by the organisation.		Risk Assessment & Treatment Plan
A.8.3	Media handling			
Objective: To prevent unauthorised disclosure, modification, removal or destruction of information stored on media.				
A.8.3.1	Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organisation.	Y	Media Handling & Removal Media Procedure
A.8.3.2	Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures.	Y	Media Handling & Secure Disposal of Media Procedure
A.8.3.3	Physical media transfer	Media containing information shall be protected against unauthorised access, misuse, or corruption during transportation.	Y	Media Handling
A.9	**Access control**			
A.9.1	Business requirements of access control			
Objective: To limit access to information and information processing facilities.				
A.9.1.1	Access control policy	An access control policy shall be established, documented and reviewed based on business and information security requirements.	Y	Access Control Policy
A.9.1.2	Access to networks and network services	Users shall only be provided with access to the network and network services that they have	Y	Access Control Policy

		been specifically authorised to use.		
A.9.2	User access management			
Objective: To ensure authorised user access and to prevent unauthorised access to systems and services				
A.9.2.1	User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	Y	User Registration & De-Registration Process
A.9.2.2	User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	Y	User Access Provisioning Process
A.9.2.3	Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.	Y	Management of Privileged Rights Authorisation Process
A.9.2.4	Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process.	Y	Secret Authentication Information Process
A.9.2.5	Review of user access rights	Asset owners shall review users' access rights at regular intervals.	Y	User Access Rights Review Process
A.9.2.6	Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Y	Removal or Adjustment of Access Rights Procedure

A.9.3	User responsibilities			
Objective: To make users accountable for safeguarding their authentication information.				
A.9.3.1	Use of secret authentication information	Users shall be required to follow the organisation's practices in the use of secret authentication information.	Y	Use of Secret Authentication Information Process
A.9.4	System and application access control			
Objective: To prevent unauthorised access to systems and applications.				
A.9.4.1	Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	Y	Access Control Policy
A.9.4.2	Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	Y	Secure Log-On Procedure
A.9.4.3	Password management system	Password management systems shall be interactive and shall ensure quality passwords.	Y	Password Control Procedure
A.9.4.4	Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	Y	Process for the Use of Privileged Utility Programs
A.9.4.5	Access control to program source code	Access to program source code shall be restricted.	Y	Access Control Policy
A.10	**Cryptography**			

A.10.1	Cryptographic controls			
Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.				
A.10.1.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for the protection of information shall be developed and implemented.	Y	Cryptographic Policy
A.10.1.2	Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	Y	Key Management Policy
A.11	**Physical and environmental security**			
A.11.1	Secure areas			
Objective: To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities.				
A.11.1.1	Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	Y	Physical & Environmental Security
A.11.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.	Y	Physical & Environmental Security
A.11.1.3	Securing offices, rooms and 8.1.3facilities	Physical security for offices, rooms and facilities shall be designed and applied.	Y	Physical & Environmental Security

A.11.1.4	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	Y	Physical & Environmental Security
A.11.1.5	Working in secure areas	Procedures for working in secure areas shall be designed and applied.	Y	Physical & Environmental Security
A.11.1.6	Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorised persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.	Y	Physical & Environmental Security
A.11.2	Equipment			
Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations.				
A.11.2.1	Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.	Y	Equipment & Equipment Siting & Protection Procedure
A.11.2.2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in	Y	Equipment

		supporting utilities.		
A.11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	Y	Equipment
A.11.2.4	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.	Y	Equipment
A.11.2.5	Removal of assets	Equipment, information or software shall not be taken off-site without prior authorisation.	Y	Equipment
A.11.2.6	Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organisation's premises.	Y	Equipment
A.11.2.7	Secure disposal or re-use of equipment	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Y	Equipment
A.11.2.8	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	Y	Equipment
A.11.2.9	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	Y	Equipment

A.12	**Operations security**			
A.12.1	Operational procedures and responsibilities			
Objective: To ensure correct and secure operations of information processing facilities.				
A.12.1.1	Documented operating procedures	Operating procedures shall be documented and made available to all users who need them.	Y	Operations Security
A.12.1.2	Change management	Changes to the organisation, business processes, information processing facilities and systems that affect information security shall be controlled.	Y	Operations Security
A.12.1.3	Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	Y	Operations Security
A.12.1.4	Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorised access or changes to the operational environment.	Y	Operations Security & Separation of Environments Procedure
A.12.2	Protection from malware			
Objective: To ensure that information and information processing facilities are protected against malware.				
A.12.2.1	Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Y	Controls Against Malware Process

A.12.3	Backup			
Objective: To protect against loss of data.				
A.12.3.1	Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	Y	Backup Policy
A.12.4	Logging and monitoring			
Objective: To record events and generate evidence.				
A.12.4.1	Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	Y	Event Log Process
A.12.4.2	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorised access.	Y	Event Log Process
A.12.4.3	Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	Y	Event Log Process
A.12.4.4	Clock synchronisation	The clocks of all relevant information processing systems within an organisation or security domain shall be synchronised to a single reference time source.	Y	Clock Synchronisation Process
A.12.5	Control of operational software			

Objective: To ensure the integrity of operational systems.				
A.12.5.1	Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.	Y	Control of Operational Software
A 12.6	Technical vulnerability management			
Objective: To prevent exploitation of technical vulnerabilities.				
A.12.6.1	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	Y	Technical Vulnerability Management
A.12.6.2	Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.	Y	Technical Vulnerability Management
A.12.7	Information systems audit considerations			
Objective: To minimise the impact of audit activities on operational systems.				
A.12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	Y	Information Systems Audit Considerations
A.13	**Communications security**			
A.13.1	Network security management			
Objective: To ensure the protection of information in networks and its supporting information processing facilities.				

A.13.1.1	Network controls	Networks shall be managed and controlled to protect information in systems and applications.	Y	Network Security Procedure
A.13.1.2	Security of network services	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	Y	Network Security Procedure
A.13.1.3	Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.	Y	Network Security Procedure
A.13.2	Information transfer			
Objective: To maintain the security of information transferred within an organisation and with any external entity.				
A.13.2.1	Information transfer policies and procedures	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	Y	Information Transfer
A.13.2.2	Agreements on information transfer	Agreements shall address the secure transfer of business information between the organisation and external parties.	Y	Information Transfer
A.13.2.3	Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	Y	Information Transfer

A.13.2.4	Confidentiality or non-disclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information shall be identified, regularly reviewed and documented.	Y	Information Transfer
A.14	**System acquisition, development and maintenance**			
A.14.1	Security requirements of information systems			
Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.				
A.14.1.1	Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	Y	System Acquisition, Development & Maintenance
A.14.1.2	Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorised disclosure and modification.	Y	Securing Application Services on Public Networks
A.14.1.3	Protecting application services transactions	Information involved in application service transactions shall be protected to prevent	Y	Protecting Application Services Transactions

		incomplete transmission, mis-routing, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.		
A.14.2	Security in development and support processes			
Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.				
A.14.2.1	Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organisation.	Y	Separation of Environments Procedure
A.14.2.2	System change control procedures	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	Y	Separation of Environments Procedure
A.14.2.3	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organisational operations or security.	Y	Separation of Environments Procedure
A.14.2.4	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	Y	Separation of Environments Procedure
A.14.2.5	Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and	Y	Separation of Environments Procedure

		applied to any information system implementation efforts.		
A.14.2.6	Secure development environment	Organisations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	Y	Separation of Environments Procedure
A.14.2.7	Outsourced development	The organisation shall supervise and monitor the activity of outsourced system development.	Y	Separation of Environments Procedure
A.14.2.8	System security testing	Testing of security functionality shall be carried out during development.	Y	Separation of Environments Procedure
A.14.2.9	System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	Y	Separation of Environments Procedure
A.14.3	Test data			
Objective: To ensure the protection of data used for testing.				
A.14.3.1	Protection of test data	Test data shall be selected carefully, protected and controlled.	Y	Separation of Environments Procedure
A.15	**Supplier relationships**			
A.15.1	Information security in supplier relationships			
Objective: To ensure protection of the organisation's assets that is accessible by suppliers.				
A.15.1.1	Information security policy for	Information security requirements for mitigating		

	supplier relationships	the risks associated with supplier's access to the organisation's assets shall be agreed with the supplier and documented.	Y	Supplier Relationships Policy
A.15.1.2	Addressing security within supplier agreements	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organisation's information.	Y	Supplier Agreement Process
A.15.1.3	Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	Y	Supplier Agreement Process
A.15.2	Supplier service delivery management			
Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.				
A.15.2.1	Monitoring and review of supplier services	Organisations shall regularly monitor, review and audit supplier service delivery.	Y	Service Management Relationship Process
A.15.2.2	Managing changes to supplier	Changes to the provision of services by suppliers,	Y	Managing Changes to Supplier Services

	services	including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.		
A.16	**Information security incident management**			
A.16.1	Management of information security incidents and improvements			
Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.				
A.16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	Y	Information Security Incident Management Policy
A.16.1.2	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	Y	Information Security Incident Management Policy
A.16.1.3	Reporting information security weaknesses	Employees and contractors using the organisation's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	Y	Information Security Incident Management Policy

A.16.1.4	Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	Y	Information Security Incident Management Policy
A.16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Y	Information Security Incident Management Policy
A.16.1.6	Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	Y	Information Security Incident Management Policy
A.16.1.7	Collection of evidence	The organisation shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	Y	Information Security Incident Management Policy
A.17	**Information security aspects of business continuity management**			
A.17.1	Information security continuity			
Objective: Information security continuity shall be embedded in the organisation's business continuity management systems.				
A.17.1.1	Planning information security continuity	The organisation shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Y	Information Security Aspects of Business Continuity Management

A.17.1.2	Implementing information security continuity	The organisation shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Y	Information Security Aspects of Business Continuity Management
A.17.1.3	Verify, review and evaluate information security continuity	The organisation shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	Y	Information Security Aspects of Business Continuity Management
A.17.2	Redundancies			
Objective: To ensure availability of information processing facilities.				
A.17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Y	Information Security Aspects of Business Continuity Management
A.18	**Compliance**			
A.18.1	Compliance with legal and contractual requirements			
Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.				
A.18.1.1	Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organisation's approach to meet these requirements shall be	Y	Compliance

		explicitly identified, documented and kept up to date for each information system and the organisation.		
A.18.1.2	Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	Y	Compliance
A.18.1.3	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorised access and unauthorised release, in accordance with legislation, regulatory, contractual and business requirements.	Y	Compliance
A.18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	Y	Compliance
A.18.1.5	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	Y	Compliance
A.18.2	Information security reviews			

Demo Company Limited		
Statement of Applicability		
ISO/IEC 27001:2013		
Issue 1	**Clause 6.1.3d**	**Authorised By:- Directors of Demo Company Limited**
Page 24 of 24	**Effective Date: 1st Nov 2021**	**Classification: - Internal**
Issue Date: 1st Nov 2021	**Last Review Date: 1st Nov 2021**	

Objective: To ensure that information security is implemented and operated in accordance with the organisational policies and procedures.				
A.18.2.1	Independent review of information security	The organisation's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	Y	Compliance
A.18.2.2	Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	Y	Compliance
A.18.2.3	Technical compliance review	Information systems shall be regularly reviewed for compliance with the organisation's information security policies and standards.	Y	Compliance