Statement of Applicability

Elaboration scope categories

- Norm requirement: we consider this point in scope due to comply to the norm.
- Organisational requirement: we consider this point to be applicable regardless of the norm.
- Customer requirement: we consider this point to be in scope to comply with the interests of our customers.
- Regulatory requirement: we consider this point to be in scope in order to comply with laws and/or regulation.

ISO 27001:2017			In scope	Implemented	Reason (not) in scope
A.5	Information security policies				
A.5.1	Management direction for securities				
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	Y	Norm requirement, Organisational requirement
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	Y	Norm requirement
A.6	Organisation of information security				
A.6.1	Internal organisation				
A.6.1.1	Information security roles and responsibilities	All information security responsibilities shall be defined and allocated	Y	Y	Norm requirement
A.6.1.2	Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organisation's assets	Y	Y	Norm requirement, Organisational requirement
A.6.1.3	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained	Y	Y	Regulatory requirement
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	Y	Norm requirement

ISO 27001:2017			In scope	Implemented	Reason (not) in scope
A.6.1.5	Information security in project management	Information security shall be addressed in project management, regardless of the type of the project	Y	Y	Norm requirement
A.6.2	Mobile devices and teleworking				
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	Y	Customer requirement, Norm requirement
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	Y	Customer requirement, Norm requirement
A.7	Human resource security				
A.7.1.	Prior to employment				
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	Y	Organisational requirement
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	Y	Customer requirement, Organisational requirement, Norm requirement
A.7.2	During employment				
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	Y	Organisational requirement
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 procedures, as relevant for their job function	Y	Y	Organisational requirement
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	Y	Organisational requirement
A.7.3	Termination and change of employment				

ISO 27001:2017			In scope	Implemented	Reason (not) in scope
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	Y	Organisational requirement, Norm requirement
A8	Asset management				
A.8.1	Responsibility for assets				
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	Y	Norm requirement
A.8.1.2	Ownership of assets	Assets maintained in the inventory shall be owned	Y	Y	Norm requirement
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	Y	Norm requirement
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 *(unless agreed otherwise)*	Y	Y	Organisational requirement
A.8.2	Information classification				
A.8.2.1	Classification of information	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification	Y	Y	Organisational requirement, Norm requirement
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	Y	Norm requirement
A.8.2.3	Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organisation	Y	Y	Norm requirement
A.8.3	Media handling				
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	Y	Norm requirement
A.8.3.2	Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures	Y	Y	Organisational requirement

ISO 27001:2017			In scope	Implemented	Reason (not) in scope
A.8.3.3	Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation	Y	Y	Norm requirement
A.9	Access control				
A.9.1	Business requirements of access control				
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	Y	Norm requirement
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 been specifically authorized to use	Y	Y	Organisational requirement
A.9.2	User access management				
A.9.2.1	User registration and deregistration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights	Y	Y	Organisational requirement
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	Y	Norm requirement
A.9.2.3	Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled	Y	Y	Norm requirement
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	Y	Norm requirement
A.9.2.5	Review of user access rights	Asset owners shall review users' access rights at regular intervals	Y	Y	Organisational requirement
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	Y	Norm requirement
A.9.3	User responsibilities				
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	Y	Organisational requirement
A.9.4	System and application access control				
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	Y	Organisational requirement
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	Y	Organisational requirement

ISO 27001:2017			In scope	Implemented	Reason (not) in scope
A.9.4.3	Password management system	Password management systems shall be interactive and shall ensure quality passwords	Y	Y	Organisational requirement
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	Y	Organisational requirement
A.9.4.5	Access control to program code	Access to program source code shall be restricted	Y	Y	Organisational requirement
A.10	Cryptography				
A.10.1	Cryptography controls				
A.10.1.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented	Y	Y	Organisational requirement
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	Y	Organisational requirement
A.11	Physical and environmental security				
A.11.1	Secure areas				
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	Y	Organisational requirement
A.11.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access	Y	Y	Organisational requirement
A.11.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied	Y	Y	Organisational requirement
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	Y	Norm requirement
A.11.1.5	Working in secure areas	Procedures for working in secure areas shall be designed and applied	Y	Y	Norm requirement
A.11.1.6	Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated form information processing facilities to avoid unauthorized access	N	N	Not applicable, no physical goods are moved as part of business
A.11.2	Equipment				
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 unauthorized access	Y	Y	Norm requirement

ISO 27001:2017			In scope	Implemented	Reason (not) in scope
A.11.2.2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities	Y	Y	Organisational requirement
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	Y	Norm requirement
A.11.2.4	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity	Y	Y	Organisational requirement
A.11.2.5	Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization	Y	Y	Norm requirement
A.11.2.6	Security 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	Y	Norm requirement
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	Y	Norm requirement
A.11.2.8	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection	Y	Y	Norm requirement
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	Y	Norm requirement, Organisational requirement
A.12	Operations security				
A.12.1	Operational procedures and responsibilities				
A.12.1.1	Documented operating procedures	Operating procedures shall be documented and made available to all users who need them	Y	Y	Organisational requirement
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	Y	Norm requirement
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	Y	Norm requirement
A.12.1.4	Separation of development, testing and operational environments	Development, testing and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment	Y	Y	Organisational requirement
A.12.2	Protection from malware				

ISO 27001:2017			In scope	Implemented	Reason (not) in scope
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	Y	Organisational requirement
A.12.3	Backup				
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	Y	Organisational requirement, Norm requirement
A.12.4	Logging and monitoring				
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	Y	Organisational requirement
A.12.4.2	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorised access	Y	Y	Organisational requirement
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	Y	Norm requirement
A.12.4.4	Clock synchronization	The clocks of all relevant information processing systems within an organisation or security domain shall be synchronized to a single reference time source	Y	Y	Norm requirement
A.12.5	Control of operational software				
A.12.5.1	Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems	Y	Y	Norm requirement
A.12.6	Technical vulnerability management				
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	Y	Norm requirement
A.12.6.2	Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented	Y	Y	Norm requirement
A.12.7	Information systems audit considerations				
A.12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to business processes	Y	Y	Norm requirement
A.13	Communications security				

ISO 27001:2017			In scope	Implemented	Reason (not) in scope
A.13.1	Network security management				
A.13.1.1	Network controls	Networks shall be managed and controlled to protect information in systems and applications	Y	Y	Organisational requirement, Norm requirement
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	Y	Norm requirement
A.13.1.3	Segregation in networks	Groups of information services, users and information systems shall be segregated on networks	Y	Y	Norm requirement
A.13.2	Information transfer				
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	Y	Norm requirement
A.13.2.2	Agreements on information transfer	Agreements shall address the secure transfer of business information between the organisation and external parties	Y	Y	Customer requirement, Organisational requirement, Norm requirement
A.13.2.3	Electronic messaging	Information involved in electronic messaging shall be appropriately protected	Y	Y	Customer requirement, Organisational requirement, Norm requirement
A.13.2.4	Confidentiality or nondisclosure 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	Y	Organisational requirement, Norm requirement
A.14	System acquisition, development and maintenance				
A.14.1	Security requirements of information systems				

ISO 27001:2017			In scope	Implemented	Reason (not) in scope
A.14.1.1	Information security 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	Y	Norm requirement
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 unauthorized disclosure and modification	Y	Y	Norm requirement
A.14.1.3	Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay	Y	Y	Organisational requirement, Norm requirement
A.14.2	Security in development and support processes				
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	Y	Organisational requirement, Norm requirement
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	Y	Organisational requirement
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	Y	Organisational requirement
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	Y	Organisational requirement
A.14.2.5	Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts	Y	Y	Norm requirement
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	Y	Organisational requirement
A.14.2.7	Outsourced development	The organisation shall supervise and monitor the activity of outsourced system development	N	N	Not applicable
A.14.2.8	System security testing	Testing of security functionality shall be carried out during development	Y	Y	Organisational requirement

ISO 27001:2017			In scope	Implemented	Reason (not) in scope
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	Y	Organisational requirement
A.14.3	Test data				
A.14.3.1	Protection of test data	Test data shall be selected carefully, protected and controlled	Y	Y	Organisational requirement
A.15	Supplier relationships				
A.15.1	Information security in supplier relationships				
A.15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets shall be agreed with the supplier and documented	Y	Y	Organisational requirement
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	Y	Organisational requirement
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	Y	Customer requirement, Organisational requirement
A.15.2	Supplier service delivery management				
A.15.2.1	Monitoring and review of supplier services	Organisations shall regularly monitor, review and audit supplier service delivery	Y	Y	Norm requirement
A.15.2.2	Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account the criticality of business information, systems and processes involved and re-assessment of risks	Y	Y	Norm requirement
A.16	Information security incident management				
A.16.1	Management of information security incidents and improvements				
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	Y	Norm requirement

ISO 27001:2017			In scope	Implemented	Reason (not) in scope
A.16.1.2	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible	Y	Y	Organisational requirement, Norm requirement
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	Y	Organisational requirement, Norm requirement
A.16.1.4	Assessment of and decision on information security incidents	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents	Y	Y	Norm requirement
A.16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures	Y	Y	Organisational requirement, Norm requirement
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	Y	Organisational requirement, Norm requirement
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	Y	Norm requirement
A.17	Information security aspects of business continuity management				
A.17.1	Information security continuity				
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	Y	Norm requirement
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 and adverse situation	Y	Y	Norm requirement
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	Y	Norm requirement
A.17.2	Redundancies				

ISO 27001:2017			In scope	Implemented	Reason (not) in scope
A.17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements	Y	Y	Organisational requirement, Norm requirement
A.18	Compliance				
A.18.1	Compliance with legal and contractual 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 explicitly identified, documented and kept up to date for each information system and the organisation	Y	Y	Regulatory requirement
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	Y	Regulatory requirement
A.18.1.3	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislator, regulatory, contractual and business requirements	Y	Y	Regulatory requirement
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	Y	Regulatory requirement, Organisational requirement
A.18.1.5	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations	Y	Y	Regulatory requirement
A.18.2	Information security reviews				
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	Y	Norm requirement
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	Y	Norm requirement

ISO 27001:2017			In scope	Implemented	Reason (not) in scope
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	Y	Norm requirement