Statement of Applicability Deloitte IT & Workplace Services v 1.0.

This statement of applicability (also reffered to as "SOA") has been developed by assessing the internal and external processes and influences to the ISMS (scope). The risks and chances of these influences on the ISMS are linked to the objectives in AnnexA of the ISO 27001:2013 standard. The following objectives and processes are present and relevant and therefore applicable to the scope of the ISMS.

#	Objective	#	Topic	Control	Applicability
5. Information Security Policies					
5.1.	**Management direction for information security** To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.	5.1.1.	Policies for information security	A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.	Applicable
		5.1.2.	Review of the policies for information security	The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Applicable
6. Organization of Information Security					
6.1.	**Internal organization** To establish a management framework to initiate and control the implementation and operation of information security within the organization.	6.1.1	Information security roles and responsibilities	All information security responsibilities should be defined and allocated.	Applicable
		6.1.2	Segregation of duties	Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	Applicable
		6.1.3	Contact with authorities	Appropriate contacts with relevant authorities should be maintained.	Applicable
		6.1.4	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.	Applicable

		6.1.5	Information security in project management	Information security should be addressed in project management, regardless of the type of the project.	Applicable
6.2.	**Mobile devices and teleworking** To ensure the security of teleworking and use of mobile devices.	6.2.1.	Mobile device policy	A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.	Applicable
		6.2.2	Teleworking	A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites.	Applicable
7. Human Resource Security					
7.1.	**Prior to employment** To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.	7.1.1	Screening	Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Applicable
		7.1.2	Terms and conditions of employment	The contractual agreements with employees and contractors should state their and the organization's responsibilities for information security.	Applicable
7.2.	**During employment** To ensure that employees and contractors are aware of and fulfil their information security responsibilities.	7.2.1	Management responsibilities	Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	Applicable
		7.2.2	Information security awareness, education and training	All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	Applicable
		7.2.3.	Disciplinary process	There should be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	Applicable

7.3.	**Termination and change of employment** To protect the organization's interests as part of the process of changing or terminating employment.	7.3.1	Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced.	Applicable
8. Asset Management					
8.1.	**Responsibility for assets** To identify organizational assets and define appropriate protection responsibilities.	8.1.1.	Inventory of assets	Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained.	Applicable
		8.1.2.	Ownership of assets	Assets maintained in the inventory should be owned.	Applicable
		8.1.3.	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities should be identified, documented and implemented.	Applicable
		8.1.4.	Return of assets	All employees and external party users should return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	Applicable
8.2.	**Information classification** To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.	8.2.1.	Classification of information	Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	Applicable
		8.2.2.	Labeling of information	An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.	Applicable
		8.2.3.	Handling of assets	Procedures for handling assets should be developed and implemented in accordance with the information classification scheme adopted by the organization.	Applicable

8.3.	**Media handling** To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.	8.3.1.	Management of removable media	Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	Applicable
		8.3.2.	Disposal of media	Media should be disposed of securely when no longer require	Applicable
		8.3.3.	Physical media transfer	Media containing information should be protected against unauthorized access, misuse or corruption during transportation.	Applicable
9. Access Control					
9.1.	**Business requirements of access control** To limit access to information and information processing facilities.	9.1.1	Access control policy	An access control policy should be established, documented and reviewed based on business and information security requirements.	Applicable
		9.1.2	Access to networks and network services	Users should only be provided with access to the network and network services that they have been specifically authorized to use.	Applicable
9.2.	**User access management** To ensure authorized user access and to prevent unauthorized access to systems and services.	9.2.1	User registration and de-registration	A formal user registration and de-registration process should be implemented to enable assignment of access rights.	Applicable
		9.2.2	User access provisioning	A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.	Applicable
		9.2.3	Management of privileged accounts	The allocation and use of privileged access rights should be restricted and controlled.	Applicable
		9.2.4	Management of secret authentication information of users	The allocation of secret authentication information should be controlled through a formal management process.	Applicable
		9.2.5.	Review of user access rights	Asset owners should review users' access rights at regular intervals.	Applicable
		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 should be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Applicable

9.3.	**User responsibilities** To make users accountable for safeguarding their authentication information.	9.3.1	Use of secret authentication information	Users should be required to follow the organization's practices in the use of secret authentication information.	Applicable
9.4.	**System and application access control** To prevent unauthorized access to systems and applications.	9.4.1	Information access restriction	Access to information and application system functions should be restricted in accordance with the access control policy.	Applicable
		9.4.2	Secure logon procedures	Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.	Applicable
		9.4.3	Password management system	Password management systems should be interactive and should ensure quality passwords.	Applicable
		9.4.4	Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.	Applicable
		9.4.5	Access control to program source code	Access to program source code should be restricted.	Applicable
10. Cryptography					
10.1.	**Cryptographic controls** To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.	10.1.1.	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information should be developed and implemented.	Applicable
		10.1.2.	Key management	A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle.	Applicable
11. Physical and Environmental Security					
11.1.	**Secure areas** To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.	11.1.1	Physical security perimeter	Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	Applicable
		11.1.2	Physical entry controls	Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Applicable
		11.1.3.	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities should be designed and applied.	Applicable

		11.1.4	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents should be designed and applied.	Applicable
		11.1.5.	Working in secure areas	Procedures for working in secure areas should be designed and applied.	Applicable
		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 should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	Applicable
11.2.	**Equipment** To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.	11.2.1	Equipment siting and protecting	Equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Applicable
		11.2.2	Supporting utilities	Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.	Applicable
		11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference or damage.	Applicable
		11.2.4	Equipment maintenance	Equipment should be correctly maintained to ensure its continued availability and integrity.	Applicable
		11.2.5	Removal of assets	Equipment, information or software should not be taken off-site without prior authorization.	Applicable
		11.2.6	Security of equipment and assets off premises	Security should be applied to off-site assets taking into account the different risks of working outside the organization's premises.	Applicable
		11.2.7	Secure disposal or re-use of equipment	All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	Applicable
		11.2.8.	Unattended user equipment	Users should ensure that unattended equipment has appropriate protection.	Applicable
		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 should be adopted.	Applicable

12. Operations security					
12.1.	**Operational procedures and responsibilities** To ensure correct and secure operations of information processing facilities.	12.1.1.	Documented operating procedures	Operating procedures should be documented and made available to all users who need them.	Applicable
		12.1.2	Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled.	Applicable
		12.1.3	Capacity management	The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	Applicable
		12.1.4	Seperation of development, testing and operational environments	Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment.	Applicable
12.2.	**Protection from malware** To ensure that information and information processing facilities are protected against malware.	12.2.1	Controls against malware	Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.	Applicable
12.3.	**Backup** To protect against loss of data.	12.3.1	Information backup	Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy.	Applicable
12.4.	**Logging and monitoring** To record events and generate evidence.	12.4.1	Event logging	Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.	Applicable
		12.4.2	Protecting of log information	Logging facilities and log information should be protected against tampering and unauthorized access.	Applicable
		12.4.3	Administrator and operator logs	System administrator and system operator activities should be logged and the logs protected and regularly reviewed.	Applicable
		12.4.4	Clock synchronisation	The clocks of all relevant information processing systems within an organization or security domain should be synchronised to a single reference time source.	Applicable
12.5.	**Control of operational software** To ensure the integrity of operational systems.	12.5.1	Installation of software on operational systems	Procedures should be implemented to control the installation of software on operational systems.	Applicable

12.6.	**Technical vulnerability management** To prevent exploitation of technical vulnerabilities.	12.6.1	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	Applicable
		12.6.2	Restrictions on software installation	Rules governing the installation of software by users should be established and implemented.	Applicable
12.7.	**Information systems audit considerations** To minimise the impact of audit activities on operational systems.	12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruptions to business processes.	Applicable
13. Communcations Security					
13.1.	**Network security management** To ensure the protection of information in networks and its supporting information processing facilities.	13.1.1	Network controls	Networks should be managed and controlled to protect information in systems and applications.	Applicable
		13.1.2.	Security of network services	Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.	Applicable
		13.1.3	Segregation in networks	Groups of information services, users and information systems should be segregated on networks.	Applicable
13.2.	**Information transfer** To maintain the security of information transferred within an organization and with any external entity.	13.2.1	Information transfer policies and procedures	Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the use of all types of communication facilities.	Applicable
		13.2.2.	Agreements on information transfer	Agreements should address the secure transfer of business information between the organization and external parties.	Applicable
		13.2.3	Electronic messaging	Information involved in electronic messaging should be appropriately protected.	Applicable
		13.2.4	Confidentiality or non-disclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, regularly reviewed and documented.	Applicable

14. System acquisition, development and maintenance					
14.1.	**Security requirements of information systems** 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.	14.1.1	Information security requirements analysis and specification	The information security related requirements should be included in the requirements for new information systems or enhancements to existing information systems.	Applicable
		14.1.2	Securing application services on public networks	Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	Applicable
		14.1.3	Protecting application services transactions	Information involved in application service transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	Applicable
14.2.	**Security in development and support processes** To ensure that information security is designed and implemented within the development lifecycle of information systems.	14.2.1	Secure development policy	Rules for the development of software and systems should be established and applied to developments within the organization.	Applicable
		14.2.2	System change control procedures	Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures.	Applicable
		14.2.3	Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or	Applicable
		14.2.4	Restrictions on changes to software packages	Modifications to software packages should be discouraged, limited to necessary changes and all changes should be strictly controlled.	Applicable
		14.2.5	Secure system engineering principles	Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts.	Applicable
		14.2.6.	Secure development environment	Organizations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	Applicable

		14.2.7	Outsourced development	The organization should supervise and monitor the activity of outsourced system development.	Applicable
		14.2.8	System security testing	Testing of security functionality should be carried out during development.	Applicable
		14.2.9.	System acceptance testing	Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions.	Applicable
14.3.	**Test data** To ensure the protection of data used for testing.	14.3.1.	Protection of test data	Test data should be selected carefully, protected and controlled.	Applicable
15. Supplier relationships					
15.1.	**Information security in supplier relationships** To ensure protection of the organization's assets that is accessible by suppliers.	15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented.	Applicable
		15.1.2.	Addressing security within supplier agreements	All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.	Applicable
		15.1.3	Information and communication technology supply chain	Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain.	Applicable
15.2.	**Supplier service delivery management** To maintain an agreed level of information security and service delivery in line with supplier agreements.	15.2.1	Monitoring and review of supplier services	Organizations should regularly monitor, review and audit supplier service delivery.	Applicable
		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, should be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.	Applicable

16. Information Security Incident Management					
16.1.	**Management of information security incidents and improvements** To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.	16.1.1	Responsibilities and procedures	Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.	Applicable
		16.1.2	Reporting information security events	Information security events should be reported through appropriate management channels as quickly as possible.	Applicable
		16.1.3.	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services should be required to note and report any observed or suspected information security weaknesses in systems or services.	Applicable
		16.1.4	Assessment of and decision on information security events	Information security events should be assessed and it should be decided if they are to be classified as information security incidents.	Applicable
		16.1.5	Response to information security incidents	Information security incidents should be responded to in accordance with the documented procedures.	Applicable
		16.1.6	Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.	Applicable
		16.1.7	Collection of evidence	The organization should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	Applicable

17. Information security aspects of business continuity management					
17.1.	**Information security continuity** Information security continuity should be embedded in the organization's business continuity management systems.	17.1.1	Planning information security continuity	The organization should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Applicable
		17.1.2	Implementing information security continuity	The organization should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Applicable
		17.1.3	Verify, review and evaluate information security continuity	The organization should 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.	Applicable
17.2.	**Redundancies** To ensure availability of information processing facilities.	17.2.1	Availability of information processing facilities	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.	Applicable
18. Compliance					
18.1.	**Compliance with legal and contractual requirements** To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.	18.1.1.	Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements should be explicitly identified, documented and kept up to date for each information system and the organization.	Applicable
		18.1.2.	Intellectual property rights	Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	Applicable

		18.1.3	Protection of records	Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.	Applicable
		18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation where applicable.	Applicable
		18.1.5.	Regulation of cryptographic controls	Cryptographic controls should be used in compliance with all relevant agreements, legislation and regulations.	Applicable
18.2.	**Information security reviews** To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.	18.2.1.	Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently at planned intervals or when significant changes occur.	Applicable
		18.2.2	Compliance with security policies and standards	Managers should 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.	Applicable
		18.2.3	Technical compliance review	Information systems should be regularly reviewed for compliance with the organization's information security policies and standards.	Applicable