IMS Statement of Applicability

Applicable ISO Standard	Control Number	Control Title	Control Objective	Applicability
	5	**Information Security Policies**		
ISO 27001	5.1	Management Direction for Information Security	Control Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.	
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	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	**Organisation of Information Security**		
ISO 27001	6.1	Internal organisation	Control Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.	
ISO 27001	6.1.1	Information security roles and responsibilities	All information security responsibilities should be defined and allocated.	Applicable
ISO 27018	6.1.1	Public cloud PII protection implementation guidance	The public cloud PII processor should designate a point of contact for use by the cloud service customer regarding the processing of PII under the contract.	Not Applicable
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	6.1.3	Contact with authorities	Appropriate contacts with relevant authorities should be maintained.	Applicable
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	6.1.5	Information security in project management	Information security should be addressed in project management, regardless of the type of the project.	Applicable
ISO 27001 ISO 27018	6.2	Mobile devices and teleworking	Control objective: To ensure the security of teleworking and use of mobile devices.	

IMS Statement of Applicability

Applicable ISO Standard	Control Number	Control Title	Control Objective	Applicability
ISO 27001 **ISO 27018**	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**
ISO 27001	6.2.2	Teleworking	A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites.	**Applicable**
ISO 27017	6.3	Relationship between Cloud Service Customer and Cloud Service Provider	Control Objective: To clarify the relationship regarding shared roles and responsibilities between the cloud service customer and the cloud service provider for information security management.	
ISO 27017	6.3.1	Shared Roles and Responsibilities within a Cloud Computing Environment	Responsibilities for shared information security roles in the use of the cloud service should be allocated to identified parties, documented, communicated and implemented by both the cloud service customer and the cloud service provider.	**Applicable**
	7	**Human Resource Security**		
ISO 27001 **ISO 27018**	7.1	Prior to employment	Control objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.	
ISO 27001 **ISO 27018**	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**
ISO 27001 **ISO 27018**	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**
ISO 27001 **ISO 27018**	7.2	During employment	Control objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.	

IMS Statement of Applicability

Applicable ISO Standard	Control Number	Control Title	Control Objective	Applicability
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	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
ISO 27018	7.2.2	Public cloud PII protection implementation guidance	Measures should be put in place to make relevant staff aware of the possible consequences on the public cloud PII processor (e.g. legal consequences, loss of business and brand or reputational damage), on the staff member (e.g. disciplinary consequences) and on the PII principal (e.g. physical, material and emotional consequences) of breaching privacy or security rules and procedures, especially those addressing the handling of PII.	Not Applicable
ISO 27018	7.2.2	Other information for public cloud PII protection	In some jurisdictions, the public cloud PII processor may be subject to legal sanctions, including substantial fines directly from the local PII protection authority. In other jurisdictions the use of International Standards such as this in setting up the contract between the public cloud PII processor and the cloud service customer should help establish a basis for contractual sanctions for a breach of security rules and procedures.	Not Applicable
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	7.3	Termination and change of employment	Control objective: To protect the organization's interests as part of the process of changing or terminating employment.	
ISO 27001 ISO 27018	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	Applicable

IMS Statement of Applicability

Applicable ISO Standard	Control Number	Control Title	Control Objective	Applicability
			defined, communicated to the employee or contractor and enforced.	
	8	**Asset Management**		
ISO 27001 **ISO 27018**	8.1	Responsibility for assets	Control objective: To identify organizational assets and define appropriate protection responsibilities.	
ISO 27001 **ISO 27018**	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**
ISO 27001 **ISO 27018**	8.1.2	Ownership of assets	Assets maintained in the inventory should be owned.	**Applicable**
ISO 27001 **ISO 27018**	8.1.3	Acceptable use of assets	Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented.	**Applicable**
ISO 27001 **ISO 27018**	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**
ISO 27017 **ISO 27018**	8.1.5	Removal of Cloud Service Customer Assets	Assets of the cloud service customer that are on the cloud service provider's premises should be removed, and returned if necessary, in a timely manner upon termination of the cloud service agreement.	**Applicable**
ISO 27001 **ISO 27018**	8.2	Information classification	Control objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.	
ISO 27001 **ISO 27018**	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**
ISO 27001 **ISO 27018**	8.2.2	Labelling 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**

IMS Statement of Applicability

Applicable ISO Standard	Control Number	Control Title	Control Objective	Applicability
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	8.3	Media handling	Control objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.	
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	8.3.2	Disposal of media	Media should be disposed of securely when no longer required, using formal procedures.	Applicable
ISO 27001 ISO 27018	8.3.3	Physical media transfer	Media containing information should be protected against unauthorized access, misuse or corruption during transportation.	Applicable
	9	**Access Control**		
ISO 27001 ISO 27018	9.1	Business requirements of access control	Control objective: To limit access to information and information processing facilities.	
ISO 27001 ISA 27018	9.1.1	Access control policy	An access control policy should be established, documented and reviewed based on business and security requirements.	Applicable
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	9.2	User access management	Control objective: To ensure authorized user access and to prevent unauthorized access to systems and services.	
ISO 27018	9.2	Public cloud PII protection implementation guidance	In the context of the service categories of the cloud computing reference architecture, the cloud service customer may be responsible for some or all aspects of access management for cloud service users under its control. Where appropriate, the public cloud PII processor should enable the cloud service customer to manage access by cloud service users under the cloud service customer's control, such as by providing	Not Applicable

Applicable ISO Standard	Control Number	Control Title	Control Objective	Applicability
			administrative rights to manage or terminate access.	
ISO 27001	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
ISO 27018	9.2.1	Public cloud PII protection implementation guidance	Procedures for user registration and de-registration should address the situation where user access control is compromised, such as the corruption or compromise of passwords or other user registration data (e.g. as a result of inadvertent disclosure).	Applicable
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	9.2.3	Management of privileged access rights	The allocation and use of privileged access rights should be restricted and controlled.	Applicable
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	9.2.5	Review of user access rights	Asset owners should review users' access rights at regular intervals.	Applicable
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	9.3	User responsibilities	Control objective: To make users accountable for safeguarding their authentication information.	
ISO 27001 ISO 27018	9.3.1	Use of secret authentication information	Users should be required to follow the organization's security practices in the use of secret authentication information.	Applicable
ISO 27001 ISO 27018	9.4	System and application access control	Control objective: To prevent unauthorized access to systems and applications.	
ISO 27001 ISO 27018	9.4.1	Information access restriction	Access to information and application system functions should be restricted in accordance with the access control policy.	Applicable

IMS Statement of Applicability

Applicable ISO Standard	Control Number	Control Title	Control Objective	Applicability
ISO 27001 ISO 27018	9.4.2	Secure log-on procedures	Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.	Applicable
ISO 27018	9.4.2	Secure Log-on procedures for Public cloud PII protection implementation guidance	Where required, the public cloud PII processor should provide secure log-on procedures for any accounts requested by the cloud service customer for cloud service users under its control.	Not Applicable
ISO 27001 ISO 27018	9.4.3	Password management system	Password management systems should be interactive and should ensure quality passwords.	Applicable
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	9.4.5	Access control to program source code	Access to program source code should be restricted.	Not Applicable
ISO 27017	A9.5	Access Control of Cloud Service Customer Data in Shared Virtual Environment	To mitigate information security risks when using the shared virtual environment of cloud computing.	
ISO 27017	A9.5.1	Segregation of Virtual Computing Environments	A cloud service customer's virtual environment running on a cloud service should be protected from other cloud service customers and unauthorized persons.	Applicable
ISO 27017	A9.5.2	Virtual Machine Hardening	Virtual machines in a cloud computing environment should be hardened to meet business needs.	Applicable
	10	**Cryptography**		
ISO 27001 ISO 27018	10.1	Cryptographic controls	Control objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity, or integrity of information.	
ISO 27001 ISO 27018	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
ISO 27018	10.1.1	Use of cryptographic controls: Public cloud PII protection implementation guidance	The public cloud PII processor should provide information to the cloud service customer regarding the circumstances in which it uses cryptography to protect the PII it processes. The public cloud PII processor	Applicable

IMS Statement of Applicability

Applicable ISO Standard	Control Number	Control Title	Control Objective	Applicability
			should also provide information to the cloud service customer about any capabilities it provides that may assist the cloud service customer in applying its own cryptographic protection.	
ISO 27001 ISO 27018	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 & Environmental Security**		
ISO 27001 ISO 27018	11.1	Secure areas	Control objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.	
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	11.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities should be designed and applied.	Applicable
ISO 27001 ISO 28018	11.1.4	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents should be designed and applied.	Applicable
ISO 27001 ISO 27018	11.1.5	Working in secure areas	Procedures for working in secure areas should be designed and applied.	Applicable
ISO 27001 ISO 27018	11.1.6	Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled and, if possible isolated from information processing facilities to avoid unauthorized access.	Applicable
ISO 27001 ISO 27018	11.2	Equipment	Control objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.	

Applicable ISO Standard	Control Number	Control Title	Control Objective	Applicability
ISO 27001	11.2.1	Equipment siting and protection	Equipment should be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Applicable
ISO 27001	11.2.2	Supporting utilities	Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.	Applicable
ISO 27001	11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference or damage.	Applicable
ISO 27001	11.2.4	Equipment maintenance	Equipment should be correctly maintained to ensure its continued availability and integrity.	Applicable
ISO 27001	11.2.5	Removal of assets	Equipment, information or software should not be taken off-site without prior authorization.	Applicable
ISO 27001	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
ISO 27001	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
ISO 27018	11,2,7	Secure disposal or re-use of equipment	For the purposes of secure disposal or re-use, equipment containing storage media that may possibly contain PII should be treated as though it does.	Applicable
ISO 27001 ISO 27018	11.2.8	Unattended user equipment	Users should ensure that unattended equipment has appropriate protection.	Applicable
ISO 27001 ISO 27018	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		
ISO 27001 ISO 27018	12.1	Operational procedures and responsibilities	Control objective: To ensure correct and secure operations of information processing facilities.	
ISO 27001 ISO 27018	12.1.1	Documented operating procedures	Operating procedures should be documented and made available to all users who need them.	Applicable

IMS Statement of Applicability

Applicable ISO Standard	Control Number	Control Title	Control Objective	Applicability
ISO 27001 ISO 27018	12.1.2	Change management	Changes to the organisation, business processes, information processing facilities and systems that affect information security should be controlled.	Applicable
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	12.1.4	Separation 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.	Not Applicable
ISO 27018	12.1.4	Separation of development, testing and operational environments	Where the use of PII for testing purposes cannot be avoided a risk assessment should be undertaken. Technical and organizational measures should be implemented to minimize the risks identified.	Applicable
ISO 27017 ISO 27018	12.1.5	Administrator's Operational Security	Procedures for administrative operations of a cloud computing environment should be defined, documented and monitored.	Applicable
ISO 27001 ISO 27018	12.2	Protection from malware	Control objective: To ensure that information and information processing facilities are protected against malware.	
ISO 27001 ISO 27018	12.2.1	Controls against malware	Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.	Applicable
ISO 27001	12.3	Backup	Control objective: To protect against loss of data.	
ISO 27001 ISO 27018	12.3.1	Information backup	Backup copies of information, software and system images should be taken and tested regularly in accordance with the agreed backup policy.	Applicable
	12.3.1	Information backup	Information processing systems based on the cloud computing model introduce additional or alternative mechanisms to off-site backups for protecting against loss of data, ensuring continuity of data processing operations, and providing the ability to restore data processing operations after a	Applicable

Applicable ISO Standard	Control Number	Control Title	Control Objective	Applicability
ISO 27018			disruptive event. Multiple copies of data in physically and/or logically diverse locations (which may be within the information processing system itself) should be created or maintained for the purposes of backup and/or recovery. PII-specific responsibilities in this respect may lie with the cloud service customer. Where the public cloud PII processor explicitly provides backup and restore services to the cloud service customer, the public cloud PII processor should provide clear information to the cloud service customer about the capabilities of the cloud service with respect to backup and restoration of the cloud service customer data. Procedures should be put in place to allow for restoration of data processing operations within a specified, documented period after a disruptive event. The back-up and recovery procedures should be reviewed at a specified, documented frequency. The use of sub-contractors to store replicated or backup copies of data being processed is covered by the controls in this International Standard applying to sub-contracted PII processing. Where physical media transfers take place this is also covered by controls in this International Standard. The public cloud PII processor should have a policy which addresses the requirements for backup of	🟩

IMS Statement of Applicability

Applicable ISO Standard	Control Number	Control Title	Control Objective	Applicability
			information and any further requirements (e.g. contractual and/or legal requirements) for the erasure of PII contained in information held for backup purposes.	
ISO 27001 **ISO 27018**	12.4	Logging and monitoring	Control objective: To record events and generate evidence.	
ISO 27001 **ISO 27018**	12.4.1	Event logging	Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.	**Applicable**
ISO 27018		Event logging for Public Cloud	A process should be put in place to review event logs with a specified, documented periodicity, to identify irregularities and propose remediation efforts. Where possible, event logs should record whether or not PII has been changed (added, modified or deleted) as a result of an event and by whom. Where multiple service providers are involved in providing service from different service categories of the cloud computing reference architecture, there may be varied or shared roles in implementing this guidance. The public cloud PII processor should define criteria regarding if, when and how log information can be made available to or usable by the cloud service customer. These procedures should be made available to the cloud service customer. Where a cloud service customer is permitted to access log records controlled by the public cloud PII processor, the public cloud PII processor should ensure that the cloud service customer can only access records that relate to that cloud service customer's activities, and cannot access any log records which relate to the activities of other cloud service customers.	

IMS Statement of Applicability

Applicable ISO Standard	Control Number	Control Title	Control Objective	Applicability
ISO 27001	12.4.2	Protection of log information	Logging facilities and log information should be protected against tampering and unauthorized access.	Applicable
ISO 27018		Protection of log information for public cloud	Log information recorded for purposes such as security monitoring and operational diagnostics may contain PII. Measures, such as controlling access (see 9.2.3), should be put in place to ensure that logged information is only used for its intended purposes. A procedure, preferably automatic, should be put in place to ensure that logged information is deleted within a specified and documented period.	
ISO 27001 ISO 27018	12.4.3	Administrator and operator logs	System administrator and system operator activities should be logged, and the logs protected and regularly reviewed.	Applicable
ISO 2700I ISO 27018	12.4.4	Clock synchronisation	The clocks of all relevant information processing systems within an organization or security domain should be synchronized to single reference time source.	Applicable
ISO 27017 ISO 27018	12.4.5	Monitoring of Cloud Services	The cloud service customer should have the capability to monitor specified aspects of the operation of the cloud services that the cloud service customer uses.	Applicable
ISO 27001 ISO 27018	12.5	Control of operational software	Control objective: To ensure the integrity of operational systems.	
ISO 27001 ISO 27018	12.5.1	Installation of software on operational systems	Procedures should be implemented to control the installation of software on operational systems.	Applicable
ISO 27001 ISO 27018	12.6	Technical vulnerability management	Control objective: To prevent exploitation of technical vulnerabilities.	
ISO 27001 ISO 27018	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
ISO 27001	12.6.2	Restrictions on software installation	Rules governing the installation of software by users should be established and implemented.	Applicable

Applicable ISO Standard	Control Number	Control Title	Control Objective	Applicability
ISO 27001	12.7	Information systems audit considerations	Control objective: To minimize the impact of audit activities on operational systems.	
ISO 27001	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	**Communications Security**		
ISO 27001 ISO 27018	13.1	Network security management	Control objective: To ensure the protection of information in networks and its supporting information processing facilities.	
ISO 27001	13.1.1	Network controls	Networks should be managed and controlled to protect information in systems and applications.	Applicable
ISO 27001	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
ISO 27001	13.1.3	Segregation in networks	Groups of information services, users and information systems should be segregated on networks.	Applicable
ISO 27017	13.1.4	Alignment of Security Management for Virtual and Physical Networks	Upon configuration of virtual networks, consistency of configurations between virtual and physical networks should be verified based on the cloud service provider's network security policy.	Applicable
ISO 27001 ISO 27018	13.2	Information transfer	Control objective: To maintain the security of information transferred within an organization and with any external entity.	
ISO 27001 ISO 27018	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
ISO 27018	13.2.1	Information Transfer policies and procedures	Whenever physical media are used for information transfer, a system should be put in place to record incoming and outgoing physical media containing PII, including the type of physical media, the authorized sender/recipients, the date and time, and the number of physical media. Where possible, cloud service	

IMS Statement of Applicability

Applicable ISO Standard	Control Number	Control Title	Control Objective	Applicability
			customers should be asked to put additional measures in place (such as encryption) to ensure that the data can only be accessed at the point of destination and not en route.	
ISO 27001 **ISO 27018**	13.2.2	Agreements on information transfer	Agreements should address the secure transfer of business information between the organization and external parties.	**Applicable**
ISO 27001 **ISO 27018**	13.2.3	Electronic messaging	Information involved in electronic messaging should be appropriately protected.	**Applicable**
ISO 27001	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	**Systems Acquisition, Development and Maintenance**		
ISO 27001 **ISO 27018**	14.1	Security requirements of information systems	Control 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.	
ISO 27001 **ISO 27018**	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**
ISO 27001 **ISO 27018**	14.1.2	Securing applications services on public and private networks	Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	**Not Applicable**
ISO 27001 **ISO 27018**	14.1.3	Protecting application services transactions	Information involved in application service transactions should be protected to prevent incomplete Tran Security Monitoring/Secession, miss-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	**Applicable**

IMS Statement of Applicability

Applicable ISO Standard	Control Number	Control Title	Control Objective	Applicability
ISO 27001 ISO 27018	14.2	Security in development and support processes	Control objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.	
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	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 security.	Applicable
ISO 27001 ISO 27018	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.	Not Applicable
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	14.2.7	Outsourced development	The organization should supervise and monitor the activity of outsourced system development.	Not Applicable
ISO 27001 ISO 27018	14.2.8	System security testing	Tests of the security functionality should be carried out during development.	Applicable
ISO 27001 ISO 27018	14.2.9	System acceptance testing	Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions.	Applicable
ISO 27001 ISO 27018	14.3	Test data	Control objective: To ensure the protection of data used for testing.	

IMS Statement of Applicability

Applicable ISO Standard	Control Number	Control Title	Control Objective	Applicability
ISO 27001 ISO 27018	14.3.1	Protection of test data	Test data should be selected carefully, protected and controlled.	Not Applicable
	15	**Supplier Relationships**		
ISO 27001 ISO 27018	15.1	Information security in supplier relationships	Control objective: To ensure protection of the organization's assets that is accessible by suppliers.	
ISO 27001 ISO 27018	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. Ref: ISO 27036-4	Applicable
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	15.2	Supplier service delivery management	Control objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.	
ISO 27001 ISO 27018	15.2.1	Monitoring and review of supplier services	Organizations should regularly monitor, review and audit supplier service delivery.	Applicable
ISO 27001 ISO 27018	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**		
ISO 27001 ISO 27018	16.1	Management of information security incidents and improvements	Control objective: To ensure a consistent and effective approach to the management of information security	

Applicable ISO Standard	Control Number	Control Title	Control Objective	Applicability
			incidents, including communication on security events and weaknesses. In the context of the whole cloud computing reference architecture, there may be shared roles in the management of information security incidents and making improvements. There may be a need for the public cloud PII processor to cooperate with the cloud service customer in implementing the controls in this subclause.	
ISO 27001	16.1.1	Incident management procedure	Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.	Applicable
ISO 27018	16.1.1	Responsibilities and procedures	An information security incident should trigger a review by the public cloud PII processor, as part of its information security incident management process, to determine if a data breach involving PII has taken place (see A.9.1). An information security event should not necessarily trigger such a review. An information security event is one that does not result in actual, or the significant probability of, unauthorized access to PII or to any of the public cloud PII processor's equipment or facilities storing PII, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful logon attempts, denial of service attacks and packet sniffing.	
ISO 27001 ISO 27018	16.1.2	Reporting information security events	Information security events should be reported through appropriate management channels as quickly as possible.	Applicable
ISO 27001 ISO 27018	16.1.3	Reporting information security weaknesses	Employees and external parties using the organisation's information systems and services should be required to note	Applicable

IMS Statement of Applicability

Applicable ISO Standard	Control Number	Control Title	Control Objective	Applicability
			and report any observed or suspected information security weaknesses in systems or services.	
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	16.1.5	Response to information security incidents	Information security incidents should be responded to in accordance with the documented procedures.	Applicable
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	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**		
ISO 27001 ISO 27018	17.1	Information security continuity	Control objective: Information security continuity should be embedded in organization’s business continuity management systems.	
ISO 27001 ISO 27018	17.1.1	Planning information security continuity	The organization should determine its requirements for information security and continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Applicable
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	17.2	Redundancies	Control objective: To ensure availability of information processing facilities.	

IMS Statement of Applicability

Applicable ISO Standard	Control Number	Control Title	Control Objective	Applicability
ISO 27001 ISO 27018	17.2.1	Availability of information processing facilities	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.	Applicable
	18	**Compliance**		
ISO 27001 ISO 27018	18.1	Compliance with legal and contractual requirements	Control objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements. Based on geographic locations	
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	18.1.2	Intellectual property rights (IPR)	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.	Not Applicable
ISO 27001 ISO 27018	18.1.3	Protection of records	Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislator, regulatory, contractual and business requirements.	Applicable
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	18.1.5	Regulation of cryptographic controls	Cryptographic controls should be used in compliance with all relevant agreements, legislation and regulations.	Applicable
ISO 27001 ISO 27018	18.2	Information security reviews	Control objective: To ensure that information security is implemented and operated in accordance with the organisational policies and procedures.	
ISO 27001	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	Applicable

IMS Statement of Applicability

Applicable ISO Standard	Control Number	Control Title	Control Objective	Applicability
			security) should be reviewed independently at planned intervals or when significant changes occur.	
ISO 27018	18.1.1	Independent review of information security on public cloud	In cases where individual cloud service customer audits are impractical or may increase risks to security (see 0.1), the public cloud PII processor should make available to prospective cloud service customers, prior to entering into, and for the duration of, a contract, independent evidence that information security is implemented and operated in accordance with the public cloud PII processor's policies and procedures. A relevant independent audit as selected by the public cloud PII processor should normally be an acceptable method for fulfilling the cloud service customer's interest in reviewing the public cloud PII processor's processing operations, provided sufficient transparency is provided.	
ISO 27001 ISO 27018	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
ISO 27001 ISO 27018	18.2.3	Technical compliance review	Information systems should be regularly reviewed for compliance with the organization's information security policies and standards.	Applicable

Additional Controls for Public Cloud Annex A

	A.1	Consent and choice		
ISO 27018	A.1	Obligation to co-operate regarding PII principals' rights	The public cloud PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them.	Applicable
ISO 27018	A.2	Purpose legitimacy and specification		
	A.2.1	Public cloud PII processor's purpose	PII to be processed under a contract should not be processed for any purpose independent of the instructions of the cloud service customer.	🟩
ISO 27018	A.2.2	Public cloud PII processor's commercial use	PII processed under a contract should not be used by the public cloud PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service.	Applicable
ISO 27018	A.3	Collection limit		
			No additional controls	
ISO 27018	A.4	Data minimization		
	A.4.1	Secure erasure of temporary files	Temporary files and documents should be erased or destroyed within a specified, documented period.	🟩
	A.5	Use, retention, and disclosure limitation		
ISO 27018	A.5.1	PII disclosure notification	The contract between the public cloud PII processor and the cloud service customer should require	🟩

			the public cloud PII processor to notify the cloud service customer, in accordance with any procedure and time periods agreed in the contract, of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited.	
ISO 27018	A.5.2	Recording of PII disclosures	Disclosures of PII to third parties should be recorded, including what PII has been disclosed, to whom and at what time.	**Applicable**
	A.6	Accuracy and quality		
			No additional controls	
	A.7			
	A.7	Disclosure of sub-contracted PII processing	The use of sub-contractors by the public cloud PII processor to process PII should be disclosed to the relevant cloud service customers before their use.	
	A.8	Individual participation and access		
			No additional controls are relevant to this privacy principle.	
	A.9	Accountability		
	A.9.1	Notification of a data breach involving PII	The public cloud PII processor should promptly notify the relevant cloud service customer in the event of any unauthorized access to PII or unauthorized access to processing equipment or facilities resulting in loss, disclosure or alteration of PII.	
	A.9.2		Copies of security policies and operating procedures should be retained for a specified, documented period upon replacement (including updating).	

	A.9.3	PII return, transfer and disposal	The public cloud PII processor should have a policy in respect of the return, transfer and/or disposal of PII and should make this policy available to the cloud service customer.	🟩
	A.10	Information Security for public cloud		
	A.10.1	Confidentiality or non-disclosure agreements	Individuals under the public cloud PII processor's control with access to PII should be subject to a confidentiality obligation.	🟩
	A.10.2	Restriction of the creation of hardcopy material	The creation of hardcopy material displaying PII should be restricted.	🟩
	A.10.3	Control and logging of data restoration	There should be a procedure for, and a log of, data restoration efforts.	🟩
	A.10.4	Protecting data on storage media leaving the premises	PII on media leaving the organization's premises should be subject to an authorization procedure and should not be accessible to anyone other than authorized personnel (e.g. by encrypting the data concerned).	🟩
	A.10.5	Use of unencrypted portable storage media and devices	Portable physical media and portable devices that do not permit encryption should not be used except where it is unavoidable, and any use of such portable media and devices should be documented.	🟩
	A.10.6	Encryption of PII transmitted over public data-transmission networks	PII that is transmitted over public data-transmission networks should be encrypted prior to transmission.	🟩
	A.10.7	Secure disposal of hardcopy materials	Where hardcopy materials are destroyed, they should be destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.	🟩

	A.10.8	Unique use of user IDs	If more than one individual has access to stored PII, then they should each have a distinct user ID for identification, authentication and authorization purposes.	🟩
	A.10.9	Records of authorized users	An up-to-date record of the users or profiles of users who have authorized access to the information system should be maintained.	🟩
	A.10.10	User ID management	De-activated or expired user IDs should not be granted to other individuals.	🟩
	A.10.11	Contract measures	Contracts between the cloud service customer and the public cloud PII processor should specify minimum technical and organizational measures to ensure that the contracted security arrangements are in place and that data are not processed for any purpose independent of the instructions of the controller. Such measures should not be subject to unilateral reduction by the public cloud PII processor.	🟩
	A.10.12	Sub-contracted PII processing	Contracts between the public cloud PII processor and any sub-contractors that process PII should specify minimum technical and organizational measures that meet the information security and PII protection obligations of the public cloud PII processor. Such measures should not be subject to unilateral reduction by the sub-contractor.	🟩
	A.10.13	Access to data on pre-used data storage space	The public cloud PII processor should ensure that whenever data storage space is assigned to a cloud	🟩

			service customer, any data previously residing on that storage space is not visible to that cloud service customer.	🟩
	A.11	Privacy compliance		
	A.11.1	Geographical location of PII	The public cloud PII processor should specify and document the countries in which PII might possibly be stored.	🟩
	A.11.2	Intended destination of PII	PII transmitted using a data-transmission network should be subject to appropriate controls designed to ensure that data reaches its intended destination.	🟩