MIPS
Diagnostics Intelligence

MIPS - Management commitment QMS and ISMS

To	MIPS Customers, Personnel Belgium, Netherlands, France, Germany, Switzerland
From	Management of MIPS
Date	August 2019

MIPS provides products and services for clinical laboratories to provide an accredited, responsive diagnostic service. Our strategy is to be and remain Europe's leading provider of clinical laboratory information systems.

Our quality management commits us to increasing customer satisfaction by continuously improving processes, products and services and by meeting international and regulatory requirements relevant to the clinical laboratory business.

With this declaration, the management of MIPS commits to support the continuous improvement and development of the established Quality Management System (QMS) and the implementation and maintenance of the Information Security Management System (ISMS) and to ensure that the activities are carried out in accordance with the process descriptions and information security regulations.

The company management ensures that the quality and security policy is defined and that the objectives derived from it are compatible with the requirements of the context of the company and the strategy. The management of MIPS provides the necessary resources to achieve these goals.

The application of the established quality management system ensures that all organizational, commercial and technical activities that affect the quality of products and services are planned, controlled and monitored.

For MIPS, information security is a matter for all employees and departments. In order to maintain the effectiveness of the ISMS, it is continuously evaluated, monitored and, if necessary, improved. This allows MIPS to develop an already high level of security awareness into a comprehensive security strategy for the future.

With the evaluation of the internal audits and the regular reporting on the results, the management of MIPS examines the effectiveness of the quality management system and the implementation of the information security management system.

Ghent, August 2019

John Lebon
CEO

MIPS liefert Produkte und Dienstleistungen für klinische Laboratorien, damit diese einen akkreditierten, reaktionsschnellen Diagnoseservice anbieten können. Unsere Strategie ist es, Europas führender Anbieter von klinischen Laborinformationssystemen zu sein und zu bleiben.

Unser Qualitätsmanagement verpflichtet uns, die Zufriedenheit unserer Kunden durch die kontinuierliche Verbesserung von Prozessen, Produkten und Dienstleistungen sowie durch die Erfüllung der internationalen und gesetzlichen Anforderungen, die für das klinische Laborgeschäft relevant sind, zu erhöhen.

Mit dieser Erklärung verpflichtet sich die Unternehmensleitung von MIPS, die kontinuierliche Verbesserung und Entwicklung des eingeführten Qualitätsmanagementsystems (QMS) und die Einführung und Aufrechterhaltung des Informationssicherheits-Managementsystems (ISMS) zu unterstützen und sicherzustellen, dass die Aktivitäten in Übereinstimmung mit den Prozessbeschreibungen und Regelungen zur Informationssicherheit durchgeführt werden.

Die Unternehmensleitung stellt sicher, dass die Qualitäts- und die Sicherheitspolitik festgelegt ist und daraus abgeleitete Ziele mit den Anforderungen aus dem Kontext des Unternehmens und der Strategie vereinbar sind. Zur Erreichung der Ziele stellt die Geschäftsführung der MIPS die erforderlichen Ressourcen zur Verfügung.

Die Anwendung des etablierten Qualitätsmanagementsystems stellt sicher, dass alle organisatorischen, kaufmännischen und technischen Aktivitäten, die Auswirkungen auf die Qualität von Produkten und Dienstleistungen haben, geplant, kontrolliert und überwacht werden.

Informationssicherheit ist für MIPS eine Angelegenheit aller Mitarbeiter und Bereiche. Um die Effektivität des ISMS zu erhalten, wird dieses kontinuierlich bewertet, überwacht und bei Bedarf verbessert. Hierdurch entwickelt MIPS ein heute bereits hohes Sicherheitsbewusstsein zu einer zukünftig umfassenden Sicherheitsstrategie.

Mit der Auswertung der internen Audits und der regelmäßigen Berichterstattung über die Ergebnisse überprüft die Unternehmensleitung von MIPS die Wirksamkeit des Qualitätsmanagementsystems und die Umsetzung des Informationssicherheits-Managementsystems.

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD
Management Service

CERTIFICATE

The Certification Body
of TÜV SÜD Management Service GmbH

certifies that

MIPS
Diagnostics Intelligence

MIPS NV

Sluisweg 2 b 5, 9000 Gent, Belgium

MIPS NV
(Netherlands)

Sluisweg 2 b 5, 9000 Gent, Belgium

MIPS Deutschland GmbH & Co. KG

Am Klingenweg 6, 65396 Walluf, Germany

MIPS Schweiz AG

Funkstrasse 106, 3084 Wabern, Switzerland

MIPS France

Cours Louis Lumière 8, 94300 Vincennes, France

has established and applies
an Information Security Management System
according to “Statement of Applicability” for

Development, implementation and service of
Laboratory systems and operations of
IT infrastructure and communication technology.

An audit was performed, Order No. **707107716**.

Proof has been furnished that the requirements
according to

ISO/IEC 27001:2013

are fulfilled. The certificate is valid from **2020-03-26** until **2023-03-25**.

Certificate Registration No.: **12 310 59753 TMS**.

Version of the statement of applicability: **2019-11-12 Ver. 1.1**.

Product Compliance Management
Munich, 2020-03-26

MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT
IAF

DAkkS
Deutsche
Akkreditierungsstelle
D-ZM-14143-01-00

MS/01-01/2019

Current as of	12/11/2019
Version	1.1
Updated by	DDB / DIK
Category	Public use

Statement of Applicability

Legend (for Selected Controls and Reasons for controls selection)

LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO/IEC 27001:2013 Controls			Control Details	Current Control (Y N TSE)	Selected Controls and Reasons for selection or inclusion (multiple columns maybe ticked)				Justification
Clause Title	N°	Control Objective/Control			LR	CO	BR/BP	RRA	
A.5 Information security policies	A.5.1	Management direction for information security							
		Objective: To provide management direction and support for information security in accordance withbusiness requirements and relevant laws and regulations.							
	A.5.1.1	Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	Yes			x		To establish information policies and to inform employees or relevant parties.
	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.	Yes			x		To check the contents of the policys and update them if necessary.
A.6 Organization of Information security	A.6.1	Internal Organization							
		Objective: To establish a management framework to initiate and control the implementation andoperation of information security within the organization.							
	A.6.1.1	Information security roles and responsibilities	All information security responsibilities shall be defined and allocated.	Yes			x	x	To inform the employees about the responsible persons and responsibilities
	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 organization's assets.	Yes			x		To reduce the possibility of unauthorized alteration or misuse of assets
	A.6.1.3	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	Yes	x			x	We maintain contacts in order to be informed about innovations and developments in our context.
	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.	Yes			x		We maintain contacts in order to be informed about the latest innivations in the field of security.
	A.6.1.5	Information security in project management	Information security shall be addressed in project management, regardless of the type of the project.	Yes			x		In order to comply with the necessary safety regulations also in projects
	A.6.2	Mobile devices and teleworking							
		To ensure the security of teleworking and use of mobile devices.							
	A.6.2.1	Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	Yes			x		To manage the risks associated with the use of mobile devices

Statement of Applicability

Category	Public use

Legend (for Selected Controls and Reasons for controls selection)

LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO/IEC 27001:2013 Controls			Control Details	Current Control (Y N TSE)	Selected Controls and Reasons for selection or inclusion (multiple columns maybe ticked)				Justification
Clause Title	N°	Control Objective/Control			LR	CO	BR/BP	RRA	
	A.6.2.2	Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	Yes			x		To manage the risks associated because there are employees in telework or homeoffice
A.7 Human resources security	A.7.1	Prior to Employment							
		To ensure that employees and contractors understand their responsibilities and are suitablefor the roles for which they are considered.							
	A.7.1.1	Screening	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Yes			x	x	HR will check the background of an applicant.
	A.7.1.2	Terms and conditions of employment	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	Yes			x		In order to strengthen our information security requirements, our contracts contain rules on information security.
	A.7.2	During Employment							
		To ensure that employees and contractors are aware of and fulfil their information securityresponsibilities.							
	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 organization.	Yes			x		The management expressly involves all employees and contractors in the implementation of the information security rules
	A.7.2.2	Information security awareness, education and training	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	Yes	x		x	x	To build and maintain adequate awareness for information security
	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.	Yes	x		x		To clarify the importance of information security and to demand compliance with the regulations.
	A.7.3	Termination or change of employment							
		To protect the organization's interests as part of the process of changing or terminatingemployment.							
	A.7.3.1	Termination or change of employment responsibilities	Responsibilities for performing employment terminaton or change of employment shall be clearly defined and assigned.	Yes			x	x	To maintain the required security measures after termination of employment
	A.8.1	Responsibility for Assets							
		To identify organizational assets and define appropriate protection responsibilities.							
	A.8.1.1	Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	Yes			x		To get an overview of the existing assets and their owners

Statement of Applicability

Category	Public use

Legend (for Selected Controls and Reasons for controls selection)

LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO/IEC 27001:2013 Controls			Control Details	Current Control (Y N TSE)	Selected Controls and Reasons for selection or inclusion (multiple columns maybe ticked)				Justification
Clause Title	N°	Control Objective/Control			LR	CO	BR/BP	RRA	
A.8 Asset Management	A.8.1.2	Ownership of assets	Assets maintained in the inventory shall be owned.	Yes			x		To get an overview of owners of the existing assets
	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.	Yes			x		To regulate the acceptable use of information and assets.
	A.8.1.4	Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	Yes			x		To regulate there return of information and assets.
	A.8.2	Information classification							
		To ensure that information receives an appropriate level of protection in accordance withits importance to the organization.							
	A.8.2.1	Classification guidelines	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	Yes			x		To classify the security needs of the information
	A.8.2.2	Information labeling and handling	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Yes			x		To ensure the safe handling of information
	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 organization.	Yes			x		To ensure the safe handling of assets
	A.8.3	Media handling							
		To prevent unauthorized disclosure, modification, removal or destruction of informationstored on media.							
	A.8.3.1	Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	Yes			x		To ensure the safe handling of removable media
	A.8.3.2	Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures.	Yes			x		To ensure the safe disposal of media
	A.8.3.3	Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	Yes			x		To ensure the safe physical transfer of media
	A.9.1	Business Requirement for Access Control							
		To limit access to information and information processing facilities.							
	A.9.1.1	Access control Policy	An access control policy shall be established, documented and reviewed based on business and information security requirements.	Yes			x	x	For the control of secure access management
	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.	Yes			x	x	To control the access authorizations
	A.9.2	User Access Management							
		To ensure authorized user access and to prevent unauthorized access to systems and services.							
	A.9.2.1	User registration and de-registration	There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.	Yes				x	To control the user registration and de-registration
	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.	Yes				x	To control the assign or revoke of Acess rights for all systems and services

Statement of Applicability

Category	Public use

Legend (for Selected Controls and Reasons for controls selection)

LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO/IEC 27001:2013 Controls			Control Details	Current Control (Y N TSE)	Selected Controls and Reasons for selection or inclusion (multiple columns maybe ticked)				Justification
Clause Title	N°	Control Objective/Control			LR	CO	BR/BP	RRA	
A.9 Access Control	A.9.2.3	Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled.	Yes				x	To control privileged acess rights.
	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.	Yes				x	To manage secret authentication information
	A.9.2.5	Review of user access rights	Asset owners shall review users' access rights at regular intervals.	Yes				x	To ensure that access permissions are correct and up-to-date
	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.	Yes				x	To ensure that no unauthorized access is made to our It-Systems
	A.9.3	User responsibilities							
		To prevent unauthorized access to systems and applications.							
	A.9.3.1	Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication information.	Yes			x		To prevent unauthorized acess and to commit employees to the responsible use of their access data
	A.9.4	System and application access control							
		To prevent unauthorized access to systems and applications.							
	A.9.4.1	Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	Yes			x	x	To prevent unauthorized access to systems and applications.
	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.	Yes			x	x	To prevent unauthorized access to systems and applications.
	A.9.4.3	Password management system	Password management systems shall be interactive and shall ensure quality passwords.	Yes			x	x	To prevent unauthorized access to systems and applications.
	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.	Yes			x	x	To prevent unauthorized access to systems and applications.
	A.9.4.5	Access control to program source code	Access to program source code shall be restricted.	Yes			x		To prevent unauthorized access to source code
A.10 Cryptography	A.10.1	Cryptographic controls							
		To ensure proper and effective use of cryptography to protect the confidentiality, authenticityand/or integrity of information.							
	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.	Yes			x	x	To protect the confidentiality, authenticity and/or integrity of information
	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.	Yes			x		To regulate the use of cryptographic keys
	A.11.1	Secure Areas							

Statement of Applicability

Category	Public use

Legend (for Selected Controls and Reasons for controls selection)

LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO/IEC 27001:2013 Controls			Control Details	Current Control (Y N TSE)	Selected Controls and Reasons for selection or inclusion (multiple columns maybe ticked)				Justification
Clause Title	N°	Control Objective/Control			LR	CO	BR/BP	RRA	
A.11 Physical and Environmental Security		To prevent unauthorized physical access, damage and interference to the organization’sinformation and information processing facilities.							
	A.11.1.1	Physical security Perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	TSE			x	x	To prevent unauthorized physical access, damage and interference to the information and processing facilities
	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.	Yes			x	x	To prevent unauthorized physical access to information processing facilities
	A.11.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied.	Yes			x	x	To prevent unauthorized physical access to our offices
	A.11.1.4	Protecting against external and environmental threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	Yes			x	x	To prevent our offices against natural disaster, accidents or malicious attacks.
	A.11.1.5	Working in secure areas	Procedures for working in secure areas shall be designed and applied.	Yes			x	x	To prevent unauthorized physical access to information processing facilities
	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 from information processing facilities to avoid unauthorized access.	Yes					To monitor the access to our company and to prevent unauthorized access
	A.11.2	Equipment security							
		To prevent loss, damage, theft or compromise of assets and interruption to the organization’soperations.							
	A.11.2.1	Equipment sitting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Yes			x	x	To reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
	A.11.2.2	Support utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Yes			x	x	In order to keep the risk of default to a minimum
	A.11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	Yes			x	x	To prevent loss, damage, theft or compromise of assets and interruption to the operations of the company
	A.11.2.4	Equipment Maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.	Yes			x	x	To ensure the availability and integrity of the equipment
	A.11.2.5	Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization.	Yes			x	x	To ensure that devices, equipment or information are not removed from the company without authorisation

Statement of Applicability

Category	Public use

Legend (for Selected Controls and Reasons for controls selection)

LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO/IEC 27001:2013 Controls			Control Details	Current Control (Y N TSE)	Selected Controls and Reasons for selection or inclusion (multiple columns maybe ticked)				Justification
Clause Title	N°	Control Objective/Control			LR	CO	BR/BP	RRA	
	A.11.2.6	Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	Yes				x	To take into account the risks associated with operation outside the company
	A.11.2.7	Secure disposal or reuse 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.	Yes			x	x	In order to comply with data protection and license protection regulations
	A.11.2.8	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	Yes			x	x	To prevent unauthorized physical access to information processing facilities
	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.	Yes			x	x	To prevent unwanted notices or destruction
A.12 Operations	A.12.1	Operational procedures and responsibilities							
		To ensure correct and secure operations of information processing facilities.							
	A.12.1.1	Documented operating procedures	Operating procedures shall be documented, maintained, and made available to all users who need them.	Yes			x		To provide all users with the necessary information.
	A.12.1.2	Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	Yes			x		To safely control organizational changes to business processes.
	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.	Yes			x		To monitor system performance and forecast future capacity requirements
	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.	Yes			x		To reduce the risks of unauthorized access or changes to the operational environment.
	A.12.2	Protection from malware							
		To ensure that information and information processing facilities are protected againstmalware.							
	A.12.2.1	Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Yes			x		To ensure that information and information processing facilities are protected against malware
	A.12.3	Back-Up							
		To protect against loss of data.							
	A.12.3.1	Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	Yes			x		To protect against loss of data.
	A.12.4	Logging and monitoring							

Statement of Applicability

Category	Public use

Legend (for Selected Controls and Reasons for controls selection)

LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO/IEC 27001:2013 Controls			Control Details	Current Control (Y N TSE)	Selected Controls and Reasons for selection or inclusion (multiple columns maybe ticked)				Justification
Clause Title	N°	Control Objective/Control			LR	CO	BR/BP	RRA	
Security		To record events and generate evidence.							
	A.12.4.1	Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	Yes			x		To record events and generate evidence.
	A.12.4.2	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	Yes			x		To protected logs against tampering and unauthorized access.
	A.12.4.3	Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	Yes			x		To record events and generate evidence.
	A.12.4.4	Clock synchronisation	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.	Yes			x		To maintain the synchronicity of processes
	A.12.5	Control of operational software							
		To ensure the integrity of operational systems.							
	A.12.5.1	Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.	Yes			x		To ensure the integrity of operational systems.
	A.12.6	Technical vulnerability management							
		To prevent exploitation of technical vulnerabilities.							
	A.12.6.1	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	Yes			x	x	To prevent exploitation of technical vulnerabilities.
	A.12.6.2	Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.	Yes			x		To control the installation of software
	A.12.7	Information systems audit considerations							
		To minimise the impact of audit activities on operational systems.							
	A.12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	Yes			x		To minimise the impact of audit activities on operational systems.
	A.13.1	Network security management							
		To ensure the protection of information in networks and its supporting information processingfacilities.							
	A.13.1.1	Network controls	Networks shall be managed and controlled to protect information in systems and applications.	Yes			x		To ensure the protection of information in networks.
	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.	Yes			x	x	To ensure the protection of information in networks and its supporting information processing facilities.
	A.13.1.3	Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.	Yes			x	x	To ensure the protection of information in networks and its supporting information processing facilities.

Statement of Applicability

Category	Public use

Legend (for Selected Controls and Reasons for controls selection)

LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO/IEC 27001:2013 Controls			Control Details	Current Control (Y N TSE)	Selected Controls and Reasons for selection or inclusion (multiple columns maybe ticked)				Justification
Clause Title	N°	Control Objective/Control			LR	CO	BR/BP	RRA	
A.13 Communications Security	A.13.2	Information transfer							
		To maintain the security of information transferred within an organization and with anyexternal entity.							
	A.13.2.1	Information transfer policies and procedures	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	Yes			x		To maintain the security of the transmission of information, inside and outside the organization
	A.13.2.2	Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties.	Yes			x		To address the secure transfer of business information between the organization and external parties.
	A.13.2.3	Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	Yes			x	x	To protect information during electronic transmission
	A.13.2.4	Confidentiality or nondisclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	Yes			x		To reflect the organization's needs for the protection of information.
	A.14.1	Security requirements of information systems							
		To ensure that information security is an integral part of information systems across theentire lifecycle. This also includes the requirements for information systems which provide servicesover public networks.							
	A.14.1.1	Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	Yes			x	x	To ensure that information security is an integral part of information systems across the company
	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.	Yes				x	To ensure that information security is an integral part of information systems across the company - both internal and external connections.
	A.14.1.3	Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	Yes				x	Protection of information during transactions using application services
	A.14.2	Security in development and support processes							
		To ensure that information security is designed and implemented within the developmentlifecycle of information systems.							
	A.14.2.1	Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization.	Yes			x	x	To ensure adoption of security rules during all development stages
	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.	Yes			x	x	To ensure adoption of security rules during all development stages

Statement of Applicability

Category	Public use

Legend (for Selected Controls and Reasons for controls selection)

LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO/IEC 27001:2013 Controls			Control Details	Current Control (Y N TSE)	Selected Controls and Reasons for selection or inclusion (multiple columns maybe ticked)				Justification
Clause Title	N°	Control Objective/Control			LR	CO	BR/BP	RRA	
A.14 System acquisition, development and maintenance	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 organizational operations or security.	Yes			x	x	To ensure adoption of security rules during all development stages
	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.	Yes			x	x	To ensure adoption of security rules during all development stages
	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.	Yes			x	x	To ensure adoption of security rules during all development stages
	A.14.2.6	Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	Yes			x	x	To ensure adoption of security rules during all development stages
	A.14.2.7	Outsourced development	The organization shall supervise and monitor the activity of outsourced system development.	Yes				x	To ensure adoption of security rules during all development stages
	A.14.2.8	System security testing	Testing of security functionality shall be carried out during development.	Yes			x	x	To ensure adoption of security rules during all development stages
	A.14.2.9	System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	Yes			x	x	To ensure adoption of security rules during all development stages
	A.14.3	Test data							
		To ensure the protection of data used for testing.							
	A.14.3.1	Protection of test data	Test data shall be selected carefully, protected and controlled.	Yes			x		To ensure the protection of data used for testing.
	A.15.1	Information security in supplier relationships							
		To ensure protection of the organization's assets that is accessible by suppliers.							
	A.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 shall be agreed with the supplier and documented.	Yes					To mitigating the risks associated with supplier's access to the organization's assets.
	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 organization's information.	Yes					To coordinate the requirements of information security for our company with the supplier and to agree regulations for this.

Statement of Applicability

Category	Public use

Legend (for Selected Controls and Reasons for controls selection)

LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO/IEC 27001:2013 Controls			Control Details	Current Control (Y N TSE)	Selected Controls and Reasons for selection or inclusion (multiple columns maybe ticked)				Justification
Clause Title	N°	Control Objective/Control			LR	CO	BR/BP	RRA	
A.15 Supplier relationships	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.	Yes					To mitigating the risks associated with information and communications technology services
	A.15.2	Supplier service delivery management							
		To maintain an agreed level of information security and service delivery in line with supplieragreements.							
	A.15.2.1	Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery.	Yes					To check the agreed level of information security and service delivery.
	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 of the criticality of business information, systems and processes involved and re-assessment of risks.	Yes			x		To maintain an agreed level of information security and service delivery in line with supplieragreements
A.16 Information security incident management	A.16.1	Management of information security incidents and improvements							
		To ensure a consistent and effective approach to the management of information securityincidents, including communication on security events and weaknesses.							
	A.16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	Yes			x		To ensure a quick and effective response to information security incidents
	A.16.1.2	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	Yes			x		To ensure a quick and effective response about information security incidents to the management
	A.16.1.3	Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	Yes			x		Ensure that employees recognize security incidents and report them immediately
	A.16.1.4	Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	Yes			x		To ensure that information security incidents are assessed and classified.
	A.16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Yes			x		To response in accordance with the documented procedures.
	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.	Yes			x		To learn and reduce the likelihood or impact of future incidents
	A.16.1.7	Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	Yes			x		Ensure the collection and preservation of information, which can serve as evidence.

Statement of Applicability

Category	Public use

Legend (for Selected Controls and Reasons for controls selection)

LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO/IEC 27001:2013 Controls			Control Details	Current Control (Y N TSE)	Selected Controls and Reasons for selection or inclusion (multiple columns maybe ticked)				Justification
Clause Title	N°	Control Objective/Control			LR	CO	BR/BP	RRA	
A.17 Information security aspects of business continuity management	A.17.1	Information security continuity							
		Information security continuity shall be embedded in the organization’s business continuitymanagement systems.							
	A.17.1.1	Planning information security continuity	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Yes			x	x	To plan the maintenance of information security
	A.17.1.2	Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Yes			x	x	To ensure the required level of continuity for information security during an adverse situation.
	A.17.1.3	Verify, review and evaluate information security continuity	The organization 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.	Yes			x	x	Verify the controls to ensure that they are valid and effective during adverse situations
	A.17.2	Redundancies							
		To essure availability of informationprocessing facilities							
	A.17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Yes					To essure availability of information processing facilities
	A.18.1	Compliance with legal and contractual requirements							
		To avoid breaches of legal, statutory, regulatory or contractual obligations related to informationsecurity and of any security requirements.							
	A.18.1.1	Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization’s approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.	Yes			x	x	To be informed about the latest laws and relevant regulations and to observe them within the company
	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.	Yes			x		To make sure that no property rights are infringed
	A.18.1.3	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.	Yes			x		To protect records from loss, destruction, falsification, unauthorized access and unauthorized release.

Statement of Applicability

Category	Public use

Legend (for Selected Controls and Reasons for controls selection)

LR: legal requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment, **TSE**: to some extent

ISO/IEC 27001:2013 Controls			Control Details	Current Control (Y N TSE)	Selected Controls and Reasons for selection or inclusion (multiple columns maybe ticked)				Justification
Clause Title	N°	Control Objective/Control			LR	CO	BR/BP	RRA	
A.18 Compliance	A.18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	Yes			x		To protect privacy in accordance with legislatory, regulatory, contractual and business requirements.
	A.18.1.5	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	Yes			x		Ensuring the application of encryption and anonymization
	A.18.2	Information security reviews							
		To ensure that information security is implemented and operated in accordance with theorganizational policies and procedures.							
	A.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) shall be reviewed independently at planned intervals or when significant changes occur.	Yes			x		In order to regularly review the implementation of information security measures
	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.	Yes			x		To ensure that the guidelines are implemented and observed by employees.
	A.18.2.3	Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization’s information security policies and standards.	Yes			x		To ensure compliance with the technical specifications