ISO_IEC 27001_2013_Cor 2_2015

Statement of Applicability

Company: *Bio-ITech B.V.*

Datum: 04/03/2021
Version: 1.0

Reason for selection

RR = Risk-based Requirement
BP = Best Practice
LR = Legal Requirement
CR = Contractual Requirement

Impl = Implemented

Bio-ITech BV
Laboratory Information Management
www.bio-itech.nl

Kieler Bocht 9
9723 JA Groningen
The Netherlands

P +31 50 72 000 55
F +31 50 21 119 16
enquiries@bio-itech.nl

IBAN: NL10 RABO 0162 6902 15
VAT: NL.8510.08.409.B.01
CC: NL 5376 5273

				Reason for selection				
#	**Title**	**Control**	**Applicable**	**RR**	**BP**	**LR**	**CR**	**Impl.**
A.5.1.1	Policy rules 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
A.5.1.2	Assessing the information security policy	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
A.6.1.1	Roles and responsibilities in information security	All information security responsibilities shall be defined and allocated.	√	√				Yes
A.6.1.2	Separation 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
A.6.1.3	Contact with government agencies	Appropriate contacts with relevant authorities shall be maintained	√	√		√		Yes
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
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
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
A.6.2.2	Telecommuting	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	√	√	√			Yes

Bio-ITech BV
Laboratory Information Management
www.bio-itech.nl

Kieler Bocht 9
9723 JA Groningen
The Netherlands

P +31 50 72 000 55
F +31 50 21 119 16
enquiries@bio-itech.nl

IBAN: NL10 RABO 0162 6902 15
VAT: NL.8510.08.409.B.01
CC: NL 5376 5273

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
A.7.1.2	Terms of employment	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	√	√	√		√	Yes
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
A.7.2.2	Awareness, education and training with regard to information security	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
A.7.2.3	Disciplinary procedure	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	√	√	√			Yes
A.7.3.1	Termination or change of responsibilities of employment	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	√	√	√			Yes
A.8.1.1	Inventory of company resources	Information, other assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	√	√	√			Yes
A.8.1.2	Ownership of company resources	Assets maintained in the inventory shall be owned.	√	√	√			Yes
A.8.1.3	Acceptable use	Rules for the acceptable use of	√	√				Yes

Bio-ITech BV
Laboratory Information Management
www.bio-itech.nl

Kieler Bocht 9
9723 JA Groningen
The Netherlands

P +31 50 72 000 55
F +31 50 21 119 16
enquiries@bio-itech.nl

IBAN: NL10 RABO 0162 6902 15
VAT: NL.8510.08.409.B.01
CC: NL 5376 5273

	of company resources	information and of assets associated with information and information processing facilities shall be identified, documented and implemented.						
A.8.1.4	Return of company resources	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
A.8.2.1	Classification of information	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.	√	√	√			Yes
A.8.2.2	Labeling information	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
A.8.2.3	Treating company resources	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	√	√				Yes
A.8.3.1	Removable media management	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	√	√				Yes
A.8.3.2	Removing media	Media shall be disposed of securely when no longer required, using formal procedures.	√	√	√			Yes
A.8.3.3	Physically transfer media	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	√	√	√			Yes
A.9.1.1	Access security policy	An access control policy shall be established, documented and reviewed based on business and information security requirements.	√	√	√			Yes
A.9.1.2	Access to networks and network	Users shall only be provided with access to the network and network services that they have been	√	√	√			Yes

Bio-ITech BV
Laboratory Information Management
www.bio-itech.nl

Kieler Bocht 9
9723 JA Groningen
The Netherlands

P +31 50 72 000 55
F +31 50 21 119 16
enquiries@bio-itech.nl

IBAN: NL10 RABO 0162 6902 15
VAT: NL.8510.08.409.B.01
CC: NL 5376 5273

	services	specifically authorized to use.						
A.9.2.1	Registration and deregistration of users	A formal user registration and de--registration process shall be implemented to enable assignment of access rights.	√	√	√			Yes
A.9.2.2	Grant users access	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
A.9.2.3	Manage special access rights	The allocation and use of privileged access rights shall be restricted and controlled.	√	√				Yes
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
A.9.2.5	Assessment of user access rights	Asset owners shall review users' access rights at regular intervals.	√	√				Yes
A.9.2.6	Revoke or change 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
A.9.3.1	Use secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication information.	√	√				Yes
A.9.4.1	Restrict access to information	Access to information and application system functions shall be restricted in accordance with the access control policy.	√	√				Yes
A.9.4.2	Secure login procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	√	√				Yes
A.9.4.3	Password management system	Password management systems shall be interactive and shall ensure quality passwords.	√	√	√			Yes
A.9.4.4	Use special	The use of utility programs that might be capable of overriding system and	√	√				Yes

Bio-ITech BV
Laboratory Information Management
www.bio-itech.nl

Kieler Bocht 9
9723 JA Groningen
The Netherlands

P +31 50 72 000 55
F +31 50 21 119 16
enquiries@bio-itech.nl

IBAN: NL10 RABO 0162 6902 15
VAT: NL.8510.08.409.B.01
CC: NL 5376 5273

	system tools	application controls shall be restricted and tightly controlled.						
A.9.4.5	Access protection based on program source code	Access to program source code shall be restricted.	√	√				Yes
A.10.1.1	Policy for the use of cryptographic control measures	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	√	√				Yes
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
A.11.1.1	Physical security zone	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	√	√	√			Yes
A.11.1.2	Physical access security	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	√	√				Yes
A.11.1.3	Secure offices, spaces and facilities	Physical security for offices, rooms and facilities shall be designed and applied.	√	√	√			Yes
A.11.1.4	Protect against external threats	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	√	√				Yes
A.11.1.5	Work in secure areas	Procedures for working in secure areas shall be designed and applied.	√	√				Yes
A.11.1.6	Loading and unloading location	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
A.11.2.1	Placement and protection of	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards,	√	√				Yes

Bio-ITech BV
Laboratory Information Management
www.bio-itech.nl

Kieler Bocht 9
9723 JA Groningen
The Netherlands

P +31 50 72 000 55
F +31 50 21 119 16
enquiries@bio-itech.nl

IBAN: NL10 RABO 0162 6902 15
VAT: NL.8510.08.409.B.01
CC: NL 5376 5273

	equipment	and opportunities for unauthorized access.						
A.11.2.2	Utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	√	√	√			Yes
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
A.11.2.4	Maintenance of equipment	Equipment shall be correctly maintained to ensure its continued availability and integrity.	√	√	√			Yes
A.11.2.5	Removal of company resources	Equipment, information or software shall not be taken off-site without prior authorization.	√	√				Yes
A.11.2.6	Security of equipment and assets outside the site	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	√	√				Yes
A.11.2.7	Safe removal 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
A.11.2.8	Unmanaged user equipment	Users shall ensure that unattended equipment has appropriate protection.	√	√	√			Yes
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
A.12.1.1	Documented operating procedures	Operating procedures shall be documented and made available to all users who need them.	√	√	√			Yes
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

Bio-ITech BV
Laboratory Information Management
www.bio-itech.nl

Kieler Bocht 9
9723 JA Groningen
The Netherlands

P +31 50 72 000 55
F +31 50 21 119 16
enquiries@bio-itech.nl

IBAN: NL10 RABO 0162 6902 15
VAT: NL.8510.08.409.B.01
CC: NL 5376 5273

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
A.12.1.4	Separation of development, test and production environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	√	√	√			Yes
A.12.2.1	Control measures against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	√	√	√			Yes
A.12.3.1	Backup of information	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	√	√	√			Yes
A.12.4.1	Register events	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	√	√	√			Yes
A.12.4.2	Protecting information in log files	Logging facilities and log information shall be protected against tampering and unauthorized access.	√	√	√			Yes
A.12.4.3	Log files of administrators and operators	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	√	√				Yes
A.12.4.4	Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to a single reference time source.	√	√				Yes
A.12.5.1	Install software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.	√	√				Yes
A.12.6.1	Management of technical vulnerabilities	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	√	√	√			Yes
A.12.6.2	Restriction for	Rules governing the installation of	√	√	√			Yes

Bio-ITech BV
Laboratory Information Management
www.bio-itech.nl

Kieler Bocht 9
9723 JA Groningen
The Netherlands

P +31 50 72 000 55
F +31 50 21 119 16
enquiries@bio-itech.nl

IBAN: NL10 RABO 0162 6902 15
VAT: NL.8510.08.409.B.01
CC: NL 5376 5273

	installing software	software by users shall be established and implemented.						
A.12.7.1	Control measures concerning audits of information systems	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	√	√				Yes
A.13.1.1	Management measures for networks	Networks shall be managed and controlled to protect information in systems and applications.	√	√	√			Yes
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
A.13.1.3	Separation in networks	Groups of information services, users and information systems shall be segregated on networks.	√	√	√			Yes
A.13.2.1	Policy and procedures for information transport	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
A.13.2.2	Agreements on information transport	Agreements shall address the secure transfer of business information between the organization and external parties.	√	√	√			Yes
A.13.2.3	Electronic reports	Information involved in electronic messaging shall be appropriately protected.	√	√	√			Yes
A.13.2.4	Confidentiality or confidentiality agreement	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
A.14.1.1	Analysis and specification of information security requirements	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	√	√				Yes

Bio-ITech BV
Laboratory Information Management
www.bio-itech.nl

Kieler Bocht 9
9723 JA Groningen
The Netherlands

P +31 50 72 000 55
F +31 50 21 119 16
enquiries@bio-itech.nl

IBAN: NL10 RABO 0162 6902 15
VAT: NL.8510.08.409.B.01
CC: NL 5376 5273

A.14.1.2	Secure 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
A.14.1.3	Protect application service transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	√	√				Yes
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
A.14.2.2	Procedures for change management with regard to systems	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	√	√				Yes
A.14.2.3	Technical assessment 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
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
A.14.2.5	Principles for engineering of secure systems	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	√	√				Yes
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

Bio-ITech BV
Laboratory Information Management
www.bio-itech.nl

Kieler Bocht 9
9723 JA Groningen
The Netherlands

P +31 50 72 000 55
F +31 50 21 119 16
enquiries@bio-itech.nl

IBAN: NL10 RABO 0162 6902 15
VAT: NL.8510.08.409.B.01
CC: NL 5376 5273

A.14.2.7	Outsourced software development	The organization shall supervise and monitor the activity of outsourced system development.	√	√				Yes
A.14.2.8	Testing system security	Testing of security functionality shall be carried out during development.	√	√	√			Yes
A.14.2.9	System acceptance tests	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions	√	√	√			Yes
A.14.3.1	Protection of test data	est data shall be selected carefully, protected and controlled.	√	√	√			Yes
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
A.15.1.2	Inclusion of security aspects in 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
A.15.1.3	Supply chain of information and communication technology	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	√	√				Yes
A.15.2.1	Monitoring and assessment of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery.	√	√				Yes
A.15.2.2	Management of changes in 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
A.16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly	√	√				Yes

Bio-ITech BV
Laboratory Information Management
www.bio-itech.nl

Kieler Bocht 9
9723 JA Groningen
The Netherlands

P +31 50 72 000 55
F +31 50 21 119 16
enquiries@bio-itech.nl

IBAN: NL10 RABO 0162 6902 15
VAT: NL.8510.08.409.B.01
CC: NL 5376 5273

		response to information security incidents.						
A.16.1.2	Reporting of information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	√	√				Yes
A.16.1.3	Reporting weaknesses in information security	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
A.16.1.4	Assessment and decision-making about 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
A.16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	√	√				Yes
A.16.1.6	Lessons learned from information security incidents	Knowledge gained from analyzing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	√	√				Yes
A.16.1.7	Collecting evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	√	√	√			Yes
A.17.1.1	Plan 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
A.17.1.2	Implement 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
A.17.1.3	Verify, assess and evaluate	The organization shall verify the established and implemented	√	√				Yes

Bio-ITech BV
Laboratory Information Management
www.bio-itech.nl

Kieler Bocht 9
9723 JA Groningen
The Netherlands

P +31 50 72 000 55
F +31 50 21 119 16
enquiries@bio-itech.nl

IBAN: NL10 RABO 0162 6902 15
VAT: NL.8510.08.409.B.01
CC: NL 5376 5273

	information security continuity	information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.						
A.17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	√	√				Yes
A.18.1.1	Determining 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
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
A.18.1.3	Protecting registrations	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.	√	√		√		Yes
A.18.1.4	Privacy and protection of personal data	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	√	√		√		Yes
A.18.1.5	Rules for the use of cryptographic control measures	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	√	√		√		Yes
A.18.2.1	Independent assessment 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	√	√	√			Yes

Bio-ITech BV
Laboratory Information Management
www.bio-itech.nl

Kieler Bocht 9
9723 JA Groningen
The Netherlands

P +31 50 72 000 55
F +31 50 21 119 16
enquiries@bio-itech.nl

IBAN: NL10 RABO 0162 6902 15
VAT: NL.8510.08.409.B.01
CC: NL 5376 5273

		occur.						
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
A.18.2.3	Assessment of technical compliance	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.	√	√				Yes

Bio-ITech BV
Laboratory Information Management
www.bio-itech.nl

Kieler Bocht 9
9723 JA Groningen
The Netherlands

P +31 50 72 000 55
F +31 50 21 119 16
enquiries@bio-itech.nl

IBAN: NL10 RABO 0162 6902 15
VAT: NL.8510.08.409.B.01
CC: NL 5376 5273