Sisukord

Statement of Applicability (SoA)

Date: 20.10.2021

- The reference table in this section shows how Directo's control objectives comply with the requirements of the current version of the standard ISO / IEC 27001: 2013. Detailed information about this standard can be found at http://www.iso.org.
- This document complies with the requirements of Annex A of the ISO / IEC27001: 2013 Security Policy.

ID	Control	Measure	Control Included
A.5	Information security policies		
A.5.1	Management direction for information security		
A.5.1.1.	Policies for information Security	Information security policy must be established by the Management Board, and be made clear to all employees and relevant external parties.	Yes
A.5.1.2	Review of the policies for information security	The information security policy must be reviewed periodically or in the event of any changes.	Yes
A.6	Organization of information security		
A.6.1	Internal Organization		
A.6.1.1	Information security roles and responsibilities	All responsibilities related to information security must be defined and assigned.	Yes
A.6.1.2	Segregation of duties	Conflicting duties and responsibilities must be separated to minimise the possibility of unauthorised or unintentional modification or misuse of the organisation's assets.	Yes
A.6.1.3	Contact with authorities	Appropriate contacts with the relevant authorities must be ensured.	Yes
A.6.1.4	Contact with special interest groups	Appropriate contacts with relevant groups of specialists or other specialised security forums and trade associations must be ensured.	Yes
A.6.1.5	Information security in project management	Project management must consider information security regardless of the project type.	Yes
A.6.2	Mobile devices and teleworking		
A.6.2.1	Mobile device policy	The appropriate policy and the security controls supporting it must be adopted to manage risks related to the use of mobile devices.	Yes
A.6.2.2	Teleworking	Information retrieved, processed or stored at teleworking locations must be protected by adopting the appropriate policy and security controls supporting it.	Yes
A.7	Human resource security		
A.7.1	Prior to employment		
A.7.1.1	Screening	The background of all job candidates must be checked in accordance with the applicable legislation, rules and ethical norms, and the scope of this checking must be in the right proportion to the requirements for the duties performed, information made available and risks perceived.	Yes

ID	Control	Measure	Control Included
A.7.1.2	Terms of conditions of employment	Contracts concluded with employees and subcontractors must formulate their and the organisation's responsibilities regarding information security.	Yes
A.7.2	During employment		
A.7.2.1	Management responsibilities	The Management must require employees and subcontractors to implement information security in accordance with the policies and procedures established in the organisation.	Yes
A.7.2.2	Information Security awareness, education and training	All employees of the organisation and also subcontractors, if applicable, must receive relevant awareness training appropriate for their duties, and regular update notifications regarding the organisation’s policies and procedures.	Yes
A.7.2.3	Disciplinary process	A formal disciplinary process must be established and communicated to the employees for the purpose of disciplining employees who have compromised information security.	Yes
A.7.3	Termination and change of employment		
A.7.3.1	Termination or change of employment responsibilities	Information security responsibilities remaining in force after terminating or modifying the employment relationship must be defined and communicated to the employees or subcontractors, and their fulfilment ensured.	Yes
A.8	Asset management		
A.8.1	Responsibility for assets		
A.8.1.1	Inventory of assets	Information assets and other assets related to information and information processing tools must be defined and an inventory list of these assets must be maintained.	Yes
A.8.1.2	Ownership of assets	The inventory list must reflect the ownership of the assets included in the list.	Yes
A.8.1.3	Acceptable use of assets	The rules establishing the acceptable use of information and information processing tools must be defined and documented.	Yes
A.8.1.4	Return of assets	All employees and external users must return all assets in their possession at the end of their employment relationship, contract or agreement.	Yes
A.8.2	Information classification		
A.8.2.1	Classification of information	Information should be classified based on legal requirements, values, criticality and sensitivity to unauthorised disclosure or modification.	Yes
A.8.2.2	Labelling of information	An appropriate procedure must be created and established for labelling information according to the information security classification scheme used in the organisation.	Yes
A.8.2.3	Handling of assets	Appropriate asset handling procedures must be created and implemented in accordance with the information classification scheme used in the organisation.	Yes

ID	Control	Measure	Control Included
A.8.3	Media handling		
A.8.3.1	Management of removable media	Guidelines must be defined for external media (memory sticks, hard disks, etc.) management.	Yes
A.8.3.2	Disposal of media	Media no longer needed must be securely and safely disposed of in accordance with formal procedures.	Yes
A.8.3.3	Physical media transfer	Media containing information must be protected against unacceptable misuse and tampering during transport.	Yes
A.9	Access Control		
A.9.1	Business requirements for access control		
A.9.1.1	Access control Policy	Access control policy must be established, documented and reviewed based on business-related and information security requirements.	Yes
A.9.1.2	Access to networks and network services	Users may only have access to the network and network services that they are specifically permitted to use.	Yes
A.9.2	User access management		
A.9.2.1	User registration and de-registration	A formal user registration and de-registration process must be established for granting access rights.	Yes
A.9.2.2	User access provisioning	A formal user registration and de-registration process must be established for all user types for granting and revoking access to all systems and services.	Yes
A.9.2.3	Management of privileged access rights	Granting and use of priority access rights must be restricted and controlled.	Yes
A9.2.4	Management of secret authentication information users	Distribution of confidential audit information must be controlled with a formal management process.	Yes
A.9.2.5	Review of user access rights	Asset owners must review the users’ access rights at regular intervals.	Yes
A.9.2.6	Removal or adjustment of access rights	Access rights to information and information processing tools granted to employees and external users must be removed upon termination of their employment relationship or contract. The rights must be adjusted when the employment relationship changes, or the contract or agreement is modified.	Yes
A.9.3	User responsibilities		
A.9.3.1	Use of secret authentication information	Users must be required to follow the organisation's practices when using secret authentication information.	Yes
A.9.4	System and application access control		
A.9.4.1	Information access restriction	Access to information and the functionalities of application systems must be restricted in accordance with the access control policy.	Yes
A.9.4.2	Secure log-on procedures	Where required by the access control policy, access to systems and applications must be controlled by secure log-on procedures.	Yes
A.9.4.3	Password management system	Password management systems must be interactive and ensure high-quality passwords.	Yes

ID	Control	Measure	Control Included
A.9.4.4	Use of privileged utility programs	The use of utilities capable of bypassing system and application security controls must be restricted and strictly controlled.	Yes
A.9.4.5	Access control to program source code	Access to the source code of the programs must be restricted.	Yes
A.10	Cryptography		
A.10.1	Cryptographic controls		
A.10.1.1	Policy of the use of cryptographic controls	A policy of the use of cryptographic controls must be created and enforced to secure information.	Yes
A.10.1.2	Key management	A policy on the use, security, and lifetime of cryptographic keys should be created and enforced over their entire lifecycle.	Yes
A.11	Physical and environmental security		
A.11.1	Secure areas		
A.11.1.1	Physical security perimeter	Security perimeters should be established in order to secure areas containing either sensitive or critical information and information processing facilities.	Yes
A.11.1.2	Physical entry controls	Secure areas must be protected by appropriate access controls to ensure that only authorised employees are allowed access.	Yes
A.11.1.3	Securing offices, rooms and facilities	Physical security must be designed and implemented for offices, rooms, and facilities.	Yes
A.11.1.4	Protecting against external and environmental threats	Physical protection must be designed and implemented against natural disasters, malicious attacks or accidents.	Yes
A.11.1.5	Working in secure areas	Procedures must be designed and adopted for working in secure areas.	Yes
A.11.1.6	Delivery and loading areas	Delivery and loading areas and other such access points and other locations where unauthorised persons might enter the premises must be monitored to prevent unauthorised access and, where possible, isolated from information processing facilities.	No
A.11.2	Equipment		
A.11.2.1	Equipment Siting & Protection	Equipment must be appropriately sited and secured to mitigate the risk of environmental hazards, risks and unauthorised access.	Yes
A.11.2.2	Supporting Utilities	Equipment must be secured or power and communication cables supporting information services must be safeguarded from data capture, interferences and damage.	Yes
A.11.2.3	Cabling Security	Power and communication cables used for carrying data or providing services must be safeguarded from data capture, interferences and damage.	Yes
A.11.2.4	Equipment Maintenance	Equipment should be correctly maintained to ensure its continued availability and integrity.	Yes
A.11.2.5	Removal of Assets	Equipment, information or software must not be taken off-premises without prior authorisation.	Yes

ID	Control	Measure	Control Included
A.11.2.6	Security of Equipment & Assets Off-Premises	The security of assets located off-premises must be implemented taking into account various risks of working outside the premises of the organisation.	Yes
A.11.2.7	Secure Disposal or Re-Use of Equipment	All units of equipment containing storage media should be inspected prior to disposal or reuse to ensure that all sensitive data and licensed software has been removed or securely overwritten.	Yes
A.11.2.8	Unattended User Equipment	Users must ensure adequate protection for their unattended equipment.	Yes
A.11.2.9	Clear Desk & Screen Policy	A clean desk policy must be adopted for paper documents and removable storage media, and a clear screen policy must be adopted for information processing tools.	Yes
A.12	Operations security		
A.12.1	Operational procedures and responsibilities		
A.12.1.1	Documented operating procedures	Operating procedures must be documented and made available to all users who need them.	Yes
A.12.1.2	Change management	Changes to the organisation, business processes, information processing tools and systems affecting information security must be controlled.	Yes
A.12.1.3	Capacity management	In order to ensure the required system performance, the use of resources must be monitored and adjusted and future capacity requirements must be prognosed.	Yes
A.12.1.4	Separation of development, testing and operational environments	To reduce the risks of unauthorised access to or modification of the operational environment, development, testing and operational environments must be separated.	Yes
A.12.2	Protection from malware		
A.12.2.1	Controls against malware	Detection, prevention and recovery controls must be adopted to protect against malware, accompanied by appropriate user awareness.	Yes
A.12.3	Backup		
A.12.3.1	Information backup	Backup copies of information, software and system images must be regularly created and tested according to the agreed-upon backup policy.	Yes
A.12.4	Logging and monitoring		
A.12.4.1	Event logging	Event logs must be created to record user activities, errors and information security events, and these must be maintained and regularly reviewed.	Yes
A.12.4.2	Protection of log information	Logging tools and logging information must be protected against tampering and unauthorised access.	Yes
A.12.4.3	Administrator and operator logs	The activities of the system administrator and system operator must be logged and these logs must be protected and regularly reviewed.	Yes
A.12.4.4	Clock synchronization	The clocks of all relevant information processing systems within the organisation or security domain must be synchronised with an agreed-upon reference source.	Yes
A.12.5	Control of operational software		

ID	Control	Measure	Control Included
A.12.5.1	Installation of software on operational systems	Procedures must be established to control the installation of software on operating systems.	Yes
A.12.6	Technical vulnerability management		
A.12.6.1	Management of technical vulnerabilities	Information on technical vulnerabilities of information systems used must be obtained promptly, exposure of the organisation to such vulnerabilities must be assessed and appropriate measures taken to mitigate the risk involved.	Yes
A.12.6.2	Restriction on software installation	Rules governing software installation must be established for the users and implemented.	Yes
A.12.7	Information systems audit considerations		
A.12.7.1	Information systems audit controls	The audit criteria and activities related to the checking of operational systems must be carefully designed and agreed upon in order to minimise interruption of operational processes.	Yes
A.13	Communications security		
A.13.1	Network security management		
A.13.1.1	Network controls	Networks must be managed and controlled to protect information contained in systems and applications.	Yes
A.13.1.2	Security of network services	Security mechanisms, service levels and management measures must be defined and included in all network service agreements, regardless of whether the services are obtained from the organisation itself or outsourced.	Yes
A.13.1.3	Segregation of networks	Groups of information services, users and information systems must be segregated within networks.	Yes
A.13.2	Information transfer		
A.13.2.1	Information transfer policies	Formal transfer policies, procedures and security controls must be established to protect information transfer via all types of communication equipment.	Yes
A.13.2.2	Agreements of information transfer	Agreements must be concluded between the organisation and external parties for transferring information related to business activities.	Yes
A.13.2.3	Electronic messaging	The information contained in electronic messaging must be handled appropriately.	Yes
A.13.2.4	Confidentiality or nondisclosure agreements	Requirements for confidentiality and non-disclosure agreements must be defined and reviewed regularly, reflecting the information protection needs of the organisation.	Yes
A.14	System acquisition, development and maintenance		
A.14.1	Security requirements of information systems		
A.14.1.1	Information security requirements analysis and specification	Information security requirements must be included in the requirements established for new information systems or improvements to existing information systems.	Yes
A.14.1.2	Securing application services on public networks	Application services running on public networks must be protected against fraud, disputes, and unauthorised disclosure and modification.	Yes

ID	Control	Measure	Control Included
A.14.1.3	Protecting application services transactions	Information contained in application services transactions must be protected against partial transfer, misrouting, unauthorised modification of messages, unauthorised disclosure, unauthorised duplication or reproduction of messages.	Yes
A.14.2	Security in development and support processes		
A.14.2.1	Secure development policy	Software and system development rules must be established and adopted for development works performed in the organisation.	Yes
A.14.2.2	System change control procedures	Changes to systems during the development lifecycle must be managed through formal change control procedures.	Yes
A.14.2.3	Technical review of applications after operating platform changes	In the event of major updates and changes to operating platforms, applications critical for the core business activities must be reviewed and tested to verify that the change does not adversely affect the activities or security of the organisation.	Yes
A.14.2.4	Restrictions on change to software packages	Changes to software packages must be controlled, restricted and regulated, as necessary.	Yes
A.14.2.5	Secure system engineering principles	Principles must be established for technological solutions of secure systems, and documented, maintained and adopted for all attempts to implement information systems.	Yes
A.14.2.6	Secure development environment	Organisations must establish and appropriately protect secure development environments for the development and integration of systems covering the entire system development lifecycle.	Yes
A.14.2.7	Outsourced development	The organisation must supervise and monitor outsourced system development works.	No
A.14.2.8	System security testing	Testing of security functionalities must be performed during the development works.	Yes
A.14.2.9	System acceptance testing	Acceptance criteria programmes and the related criteria must be established for new information systems, updates and new versions.	Yes
A.14.3	Test data		
A.14.3.1	Protection of test data	Test data must be carefully selected, protected and controlled.	Yes
A.15	Supplier relationships		
A.15.1	Information security in supplier relationships		
A.15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with the supplier's access to the organisation's assets must be agreed with the supplier and documented.	Yes
A.15.1.2	Addressing security within supplier agreements	Relevant information security requirements must be established and agreed with each supplier who accesses the organisation's information and processes or creates IT infrastructure components for it.	Yes

ID	Control	Measure	Control Included
A.15.1.3	Information and communication technology supply chain	Agreements with suppliers must include requirements to address information security risks related to the supply chain of ICT services and products.	Yes
A.15.2	Supplier service delivery management		
A.15.2.1	Monitoring and review of supplier services	Organisations must regularly monitor, review and audit the delivery of supplier services.	Yes
A.15.2.2	Managing changes to supplier services	Changes in the provision of services by suppliers, including the maintenance and improvement of existing information security policies, procedures and controls, must be managed, focusing on the criticality of the relevant enterprise information and production systems and processes, as well as the reassessment of risks.	Yes
A.16	Information security incident management		
A.16.1	Management of information security incidents & improvements		
A.16.1.1	Responsibilities and procedures	Managing responsibilities and procedures must be established to ensure a swift, effective and proper response to information security incidents.	Yes
A.16.1.2	Reporting information security events	Information security events should be reported as soon as possible via appropriate administrative channels.	Yes
A.16.1.3	Reporting information security weaknesses	Employees and subcontractors using the organisation's information systems and services should be required to notice vulnerabilities of the systems or services and report any occurrences or vulnerabilities.	Yes
A.16.1.4	Assessment of and decision on information security events	Information security events should be assessed and their classification as information security incidents should determined.	Yes
A.16.1.5	Response to information security incidents	Information security incidents must be responded to in accordance with documented procedures.	Yes
A.16.1.6	Learning from information security incidents	Information obtained from analysing and resolving information security incidents must be used to reduce the possibility or impact of future incidents.	Yes
A.16.1.7	Collection of evidence	The organisation must define and implement procedures for the identification, collection, acquisition and storage of information suitable to be used as evidence.	Yes
A.17	Information security aspects of business continuity management		
A.17.1	Information security continuity		
A.17.1.1	Planning information security continuity	The organisation must define its requirements for security and the continuity of information security management in adverse situations, such as a crisis or disaster.	Yes
A.17.1.2	Implementing information security continuity	The organisation must establish, document, implement and maintain processes to ensure the required level of information security continuity in adverse situations.	Yes

ID	Control	Measure	Control Included
A.17.1.3	Verify, review and evaluate information security continuity	The organisation must review the information security continuity controls established and implemented at regular intervals to ensure that they are adequate and effective in adverse situations.	Yes
A.17.2	Redundancies		
A.17.2.1	Availability of information processing facilities	Information processing tools should be implemented with sufficient duplication to meet availability requirements.	Yes
A.18	Compliance		
A.18.1	Compliance with legal and contractual requirements		
A.18.1.1	Identification of applicable legislation and contractual requirements	All applicable requirements arising from legislation and contracts, and the method used by the organisation to comply with them must be clearly outlined, documented and kept appropriate for every information system and the organisation.	Yes
A.18.1.2	Intellectual property rights	Appropriate procedures must be adopted to ensure compliance with legislative, regulatory and contractual requirements and the requirements of the core business.	Yes
A.18.1.3	Protection of records	Datasets must be protected against loss, destruction, falsification, unauthorised access, and disclosure in accordance with legislation, regulations and contractual obligations.	Yes
A.18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personal data must be ensured in accordance with applicable legislation and regulations where appropriate.	Yes
A.18.1.5	Regulation of cryptographic controls	Cryptographic security controls must be used in accordance with all applicable agreements, legislation and rules.	Yes
A.18.2	Information security reviews		
A.18.2.1	Independent review of information security	An independent review of the organisation's approach to the management and implementation of information security (policies, procedures, rules) should be carried out at scheduled intervals or in the event of significant changes.	Yes
A.18.2.2	Compliance with security policies and standards	Managers must regularly review the compliance of information processing and procedures with relevant security policies and other requirements within their area of responsibility.	Yes
A.18.2.3	Technical compliance review	The compliance of information systems with the organisation’s guiding information security policy and standards must be regularly checked.	Yes