Document Classification: Public

Statement of Applicability, Version 2.0, 4 May 2021

Legend for Reasons for Controls Selection

LR: Legal Requirements,CO: Contractual Obligations,BR/BP: Business Requirements/Adopted Best Practices,RRA: Results of Risk Assessment

Section	Information security control	Reference	Applicable
A5	**Information security policies**		
A5.1	**Management direction for information security**		
A5.1.1	Policies for information security	Information_Security_Policy; ISMS Manual; Security Concept	Yes
A5.1.2	Review of the policies for information security	Document_and_Policy Management	Yes
A6	**Organization of information security**		
A6.1	**Internal organization**		
A6.1.1	Information security roles and responsibilities	ISMS Manual; Information_Security_Policy; Job descriptions	Yes
A6.1.2	Segregation of duties	ISMS Manual; Information_Security_Policy; Access_Control_Policy	Yes
A6.1.3	Contact with authorities	Computer_Security_Incident_Response_Plan (Annex II)	Yes
A6.1.4	Contact with special interest groups	Computer_Security_Incident_Response_Plan (Annex II)	Yes
A6.1.5	Information security in project management	Information Security Risk Management Policy; Software Development Process	Yes
A6.2	**Mobile devices and teleworking**		
A6.2.1	Mobile device policy	Mobile_Device_Policy	Yes
A6.2.2	Teleworking	Teleworking_Policy	Yes
A7	**Human resource security**		
A7.1	**Prior to employment**		
A7.1.1	Screening	On_Off Boarding Checkliste	Yes
A7.1.2	Terms and conditions of employment	Safety io Arbeitsvertrag_AT	Yes
A7.2	**During employment**		
A7.2.1	Management responsibilities	Information_Security_Policy; ISMS Manual	Yes
A7.2.2	Information security awareness, education and training	ISMS Manual	Yes
A7.2.3	Disciplinary process	Information_Security_Policy; Progressive Discipline Policy	Yes
A7.3	**Termination and change of employment**		
A7.3.1	Termination or change of employment responsibilities	Safety io Arbeitsvertrag_AT	Yes
A8	**Asset management**		
A8.1	**Responsibility for assets**		
A8.1.1	Inventory of assets	ISMS Asset Register	Yes
A8.1.2	Ownership of assets	ISMS Asset Register	Yes
A8.1.3	Acceptable use of assets	Acceptable_Use_Policy	Yes
A8.1.4	Return of assets	Supplier_Security_Policy; Safety io Arbeitsvertrag_AT	Yes
A8.2	**Information classification**		
A8.2.1	Classification of information	Data_Classification_Policy	Yes
A8.2.2	Labelling of information	Security Concept; Data_Classification_Policy	Yes
A8.2.3	Handling of assets	Data_Classification_Policy; Acceptable_Use_Policy;	Yes
A8.3	**Media handling**		
A8.3.1	Management of removable media	Mobile_Device_Policy	Yes
A8.3.2	Disposal of media	Security Concept	Yes
A8.3.3	Physical media transfer	Security Concept	Yes
A9	**Access control**		
A9.1	**Business requirements of access control**		
A9.1.1	Access control policy	Access_Control_Policy	Yes
A9.1.2	Access to networks and network services	Access_Control_Policy; Teleworking_Policy; Security Concept	Yes
A9.2	**User access management**		
A9.2.1	User registration and de-registration	Access_Control_Policy; Administrators_Policy	Yes
A9.2.2	User access provisioning	Access_Control_Policy; Administrators_Policy	Yes
A9.2.3	Management of privileged access rights	Access_Control_Policy; Administrators_Policy	Yes
A9.2.4	Management of secret authentication information of users	Password_Policy; Acceptable_Use_Policy	Yes
A9.2.5	Review of user access rights	Access_Control_Policy	Yes
A9.2.6	Removal or adjustment of access rights	Access_Control_Policy	Yes
A9.3	**User responsibilities**		
A9.3.1	Use of secret authentication information	Password_Policy; Access_Control_Policy	Yes
A9.4	**System and application access control**		
A9.4.1	Information access restriction	Data_Classification_Policy Access_Control_Policy	Yes
A9.4.2	Secure log-on procedures	Access_Control_Policy	Yes
A9.4.3	Password management system	Password_Policy	Yes

Section	Information security control	Reference	Applicable
A9.4.4	Use of privileged utility programs	Access Control Policy; Administrators Policy	Yes
A9.4.5	Access control to program source code	Access_Control_Policy	Yes
A10	**Cryptography**		
A10.1	**Cryptographic controls**		
A10.1.1	Policy on the use of cryptographic controls	Cryptographic_Key_Management_Policy	Yes
A10.1.2	Key management	Cryptographic_Key_Management_Policy	Yes
A11	**Physical and environmental security**		
A11.1	**Secure areas**		
A11.1.1	Physical security perimeter	Security Concept	Yes
A11.1.2	Physical entry controls	Access_Control_Policy	Yes
A11.1.3	Securing offices, rooms and facilities	Security Concept; Access_Control_Policy	Yes
A11.1.4	Protecting against external and environmental threats	Security Concept	Yes
A11.1.5	Working in secure areas	Security Concept	Yes
A11.1.6	Delivery and loading areas	Security Concept	Yes
A11.2	**Equipment**		
A11.2.1	Equipment siting and protection	Security Concept	Yes
A11.2.2	Supporting utilities	Security Concept	Yes
A11.2.3	Cabling security	Security Concept	Yes
A11.2.4	Equipment maintenance	Security Concept	Yes
A11.2.5	Removal of assets	Security Concept	Yes
A11.2.6	Security of equipment and assets off-premises	Security Concept	Yes
A11.2.7	Secure disposal or reuse of equipment	Security Concept	Yes
A11.2.8	Unattended user equipment	Clear_Desk_And_Clear_Screen_Policy	Yes
A11.2.9	Clear desk and clear screen policy	Clear_Desk_And_Clear_Screen_Policy	Yes
A12	**Operations security**		
A12.1	**Operational procedures and responsibilities**		
A12.1.1	Documented operating procedures	Security Concept; Administrators Policy	Yes
A12.1.2	Change management	Software Development Process; Security Concept	Yes
A12.1.3	Capacity management	Software Development Process	Yes
A12.1.4	Separation of development, testing and operational environments	Software Development Process	Yes
A12.2	**Protection from malware**		
A12.2.1	Controls against malware	Security Concept	Yes
A12.3	**Backup**		
A12.3.1	Information backup	Security Concept; Backup Overview	Yes
A12.4	**Logging and monitoring**		
A12.4.1	Event logging	Security Concept	Yes
A12.4.2	Protection of log information	Security Concept	Yes
A12.4.3	Administrator and operator logs	Security Concept	Yes
A12.4.4	Clock synchronisation	Security Concept	Yes
A12.5	**Control of operational software**		
A12.5.1	Installation of software on operational systems	Administrators Policy; Security Concept	Yes
A12.6	**Technical vulnerability management**		
A12.6.1	Management of technical vulnerabilities	Vulnerability_Management_Policy	Yes
A12.6.2	Restrictions on software installation	Mobile Device Policy; Acceptable Use Policy	Yes
A12.7	**Information systems audit considerations**		
A12.7.1	Information systems audit controls	Security Concept	Yes
A13	**Communications security**		
A13.1	**Network security management**		

Section	Information security control	Reference	Applicable
A13.1.1	Network controls	Security Concept	Yes
A13.1.2	Security of network services	Security Concept	Yes
A13.1.3	Segregation in networks	Security Concept	Yes
A13.2	**Information transfer**		
A13.2.1	Information transfer policies and procedures	Data_Classification_Policy	Yes
A13.2.2	Agreements on information transfer	Data_Classification_Policy Supplier_Security_Policy	Yes
A13.2.3	Electronic messaging	Data_Classification_Policy	Yes
A13.2.4	Confidentiality or nondisclosure agreements	Supplier_Security_Policy; Safety io Work for Hire Agreement; Safety io Arbeitsvertrag_AT	Yes
A14	**System acquisition, development & maintenance**		
A14.1	**Security requirements of information systems**		
A14.1.1	Information security requirements analysis and specification	Software Development Process	Yes
A14.1.2	Securing application services on public networks	Software Development Process	Yes
A14.1.3	Protecting application services transactions	Software Development Process	Yes
A14.2	**Security in development and support processes**		
A14.2.1	Secure development policy	Software Development Process	Yes
A14.2.2	System change control procedures	Security Concept	Yes
A14.2.3	Technical review of applications after operating platform changes	Security Concept	Yes
A14.2.4	Restrictions on changes to software packages	Security Concept	Yes
A14.2.5	Secure system engineering principles	Software Development Process	Yes
A14.2.6	Secure Development Environment	Security Concept	Yes
A14.2.7	Outsourced development	Software Development Process	Yes
A14.2.8	System security testing	Software Development Process	Yes
A14.2.9	System acceptance testing	Software Development Process	Yes
A14.3	**Test data**		
A14.3.1	Protection of test data	Software Development Process	Yes
A15	**Supplier relationships**		
A15.1	**Information security in supplier relationships**		
A15.1.1	Information security policy for supplier relationships	Supplier_Security_Policy	Yes
A15.1.2	Addressing security within supplier agreements	Supplier_Security_Policy; AWS_NDA; Safety io Work for Hire Agreement	Yes
A15.1.3	ICT supply chain	Supplier_Security_Policy; Third Party Review Process; Vendor Security Questionnaire; Safety io Work for Hire Agreement	Yes
A15.2	**Supplier service delivery management**		
A15.2.1	Monitoring and review of supplier services	Supplier_Security_Policy	Yes
A15.2.2	Managing changes to supplier services	Supplier_Security_Policy	Yes
A16	**Information security incident management**		
A16.1	**Management of information security incidents & improvements**		
A16.1.1	Responsibilities and procedures	Computer_Security_Incident_Response_Plan	Yes
A16.1.2	Reporting information security events	Computer_Security_Incident_Response_Plan	Yes
A16.1.3	Reporting information security weaknesses	Computer_Security_Incident_Response_Plan	Yes
A16.1.4	Assessment of and decision on information security events	Computer_Security_Incident_Response_Plan	Yes
A16.1.5	Response to information security incidents	Computer_Security_Incident_Response_Plan	Yes
A16.1.6	Learning from information security incidents	Computer_Security_Incident_Response_Plan	Yes
A16.1.7	Collection of evidence	Computer_Security_Incident_Response_Plan	Yes
A17	**Information security aspects of BCM**		
A17.1	**Information security continuity**		
A17.1.1	Planning information security continuity	Security Concept	Yes
A17.1.2	Implementing information security continuity	Security Concept	Yes
A17.1.3	Verify, review and evaluate information security continuity	Security Concept	Yes
A17.2	**Redundancies**		
A17.2.1	Availability of information processing facilities	Security Concept	Yes
A18	**Compliance**		
A18.1	**Compliance with legal and contractual requirements**		
A18.1.1	Identification of applicable legislation and contractual requirements	Legal, regulatory and contractual requirements	Yes
A18.1.2	Intellectual property rights	NPD R4 Intellectual Property	Yes
A18.1.3	Protection of records	Data Classification Policy	Yes
A18.1.4	Privacy and protection of personally identifiable information	Legal, regulatory and contractual requirements; Data Classification Policy	Yes
A18.1.5	Regulation of cryptographic controls	Security Concept	Yes
A18.2	**Information security reviews**		
A18.2.1	Independent review of information security	ISMS Manual; Internal Audit Process	Yes
A18.2.2	Compliance with security policies and standards	ISMS Manual; Internal Audit Process	Yes
A18.2.3	Technical compliance review	ISMS Manual; Internal Audit Process	Yes