cirrus

The no-compromise online exam platform .

Statement of Applicability: Cirrus B.V.

Version: 1.2, *current as of 18-05-2022* Classification : Public

Legend (for Selected Controls and Reasons for controls selection) Source: Cirrus_Security_Framework_And_SOA_2013

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 Annex A controls			Applicable	Implemented	Reasson for exclusion	Selected Controls and Reasons for Selection			
Clause	Sec	Control Objective/Control				LR	CO	BR/BP	RRA
A5 Security Policies	A.5.1	Management direction for information security							
	A5.1.1	Policies for information	Yes	Yes				✓	✓
	A5.1.2	Review of the policies for information security	Yes	Yes				✓	✓
A6 Organisation of information security	A6.1	Internal organisation							
	A6.1.1	Information security roles and responsibilities	Yes	Yes				✓	✓
	A6.1.2	Segregation of duties	Yes	Yes				✓	✓
	A6.1.3	Contact with authorities	Yes	Yes				✓	✓
	A6.1.4	Contact with special interest groups	Yes	Yes				✓	✓
	A6.1.5	Information security in project management	Yes	Yes				✓	✓
	A6.2	Mobile devices and teleworking							
	A6.2.1	Mobile device policy	Yes	Yes				✓	✓
	A6.2.2	Teleworking	Yes	Yes				✓	✓
A7 Human resource security	A7.1	Prior to employment							
	A7.1.1	Screening	Yes	Yes				✓	✓
	A7.1.2	Terms and conditions of employment	Yes	Yes				✓	✓
	A7.2	During employment							
	A7.2.1	Management responsibilities	Yes	Yes				✓	✓
	A7.2.2	Information security awareness, education and training	Yes	Yes				✓	✓
	A7.2.3	Disciplinary process	Yes	Yes				✓	✓
	A7.3	Termination and change of employment							
	A7.3.1	Termination or change of employment responsibilities	Yes	Yes				✓	✓
A8 Asset management	A8.1	Responsibility for assets							
	A8.1.1	Inventory of assets	Yes	Yes				✓	✓
	A8.1.2	Ownership of assets	Yes	Yes				✓	✓
	A8.1.3	Acceptable use of assets	Yes	Yes				✓	✓
	A8.1.4	Return of assets	Yes	Yes				✓	✓
	A8.2	Information classification							
	A8.2.1	Classification of information	Yes	Yes				✓	✓
	A8.2.2	Labeling of information	Yes	Yes				✓	✓
	A8.2.3	Handling of assets	Yes	Yes				✓	✓
	A8.3	Media handling							
	A8.3.1	Management of removable media	Yes	Yes				✓	✓
	A8.3.2	Disposal of media	Yes	Yes				✓	✓
	A8.3.3	Physical media transfer	Yes	Yes				✓	✓
A9 Access control	A9.1	Business requirements of access control							
	A9.1.1	Access control policy	Yes	Yes				✓	✓
	A9.1.2	Access to networks and network services	Yes	Yes				✓	✓
	A9.2	User access management							
	A9.2.1	User registration and de-registration	Yes	Yes				✓	✓
	A9.2.2	User access provisioning	Yes	Yes				✓	✓
	A9.2.3	Management of privileged access rights	Yes	Yes				✓	✓
	A9.2.4	Management of secret authentication information of users	Yes	Yes				✓	✓
	A9.2.5	Review of user access rights	Yes	Yes				✓	✓
	A9.2.6	Removal or adjustment of access rights	Yes	Yes				✓	✓
	A9.3	User responsibilities							
	A9.3.1	Use of secret authentication information	Yes	Yes				✓	✓
	A9.4	System and application access control							
	A9.4.1	Information access restriction	Yes	Yes				✓	✓
	A9.4.2	Secure log-on procedures	Yes	Yes				✓	✓
	A9.4.3	Password management system	Yes	Yes				✓	✓
	A9.4.4	Use of privileged utility programs	Yes	Yes				✓	✓
	A9.4.5	Access control to program source code	Yes	Yes				✓	✓
A10 Cryptography	A10.1	Cryptographic controls							
	A10.1.1	Policy on the use of cryptographic controls	Yes	Yes		✓		✓	✓
	A10.1.2	Key management	Yes	Yes				✓	✓
A11 Physical and environmental security	A11.1	Secure areas							
	A11.1.1	Physical security perimeter	Yes	Yes					✓
	A11.1.2	Physical entry controls	Yes	Yes					✓
	A11.1.3	Securing office, room and facilities	Yes	Yes					✓
	A11.1.4	Protecting against external end environmental threats	Yes	Yes					✓
	A11.1.5	Working in secure areas	No	N/A	Applies to our hosting partner with servers/backups. Cirrus policies enable secure working in public				
	A11.1.6	Delivery and loading areas	No	N/A	Applies to our hosting partner. Cirrus has no offices with servers/backups, nor unsecure data due to our data handling policy				
	A11.2	Equipment							
	A11.2.1	Equipment siting and protection	Yes	Yes					✓
	A11.2.2	Supporting utilities	No	N/A	Cirrus has no infrastructure of its own				
	A11.2.3	Cabling security	No	N/A	Cirrus has no infrastructure of its own				

Statement of Applicability: Cirrus B.V.

Version: 1.2, *current as of 18-05-2022* Classification : Public

Legend (for Selected Controls and Reasons for controls selection) Source: Cirrus_Security_Framework_And_SOA_2013

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 Annex A controls			Applicable	Implemented	Reasson for exclusion	Selected Controls and Reasons for Selection			
Clause	Sec	Control Objective/Control				LR	CO	BR/BP	RRA
	A11.2.4	Equipment maintenance	Yes	Yes					✓
	A11.2.5	Removal of assets	Yes	Yes					✓
	A11.2.6	Security of equipment and assets off-premises	Yes	Yes					✓
	A11.2.7	Secure disposal or re-use of equipment	Yes	Yes					✓
	A11.2.8	Unattended user equipment	Yes	Yes					✓
	A11.2.9	Clear desk and clear screen policy	Yes	Yes					✓
A12 Operations security	A12.1	Operational procedures and responsibilities							
	A12.1.1	Documented operating procedures	Yes	Yes				✓	✓
	A12.1.2	Change management	Yes	Yes				✓	✓
	A12.1.3	Capacity management	Yes	Yes			✓	✓	✓
	A12.1.4	Separation of development, testing and operational environments	Yes	Yes				✓	✓
	A12.2	Protection from malware							
	A12.2.1	Controls against malware	Yes	Yes				✓	✓
	A12.3	Backup							
	A12.3.1	Information backup	Yes	Yes			✓	✓	✓
	A12.4	Logging and monitoring							
	A12.4.1	Event logging	Yes	Yes				✓	✓
	A12.4.2	Protection of log information	Yes	Yes				✓	✓
	A12.4.3	Administrator and operator logs	Yes	Yes				✓	✓
	A12.4.4	Clock synchronisaton	Yes	Yes				✓	✓
	A12.5	Control of operational software							
	A12.5.1	Installation of software on operational systems	Yes	Yes				✓	✓
	A12.6	Technical vulnerability management							
	A12.6.1	Management of technical vulnerabilities	Yes	Yes				✓	✓
	A12.6.2	Restrictions on software installation	Yes	Yes				✓	✓
	A12.7	Information systems audit considerations							
	A12.7.1	Information systems audit controls	Yes	Yes				✓	✓
A13 Communications security	A13.1	Network security management							
	A13.1.1	Network controls	Yes	Yes			✓	✓	✓
	A13.1.2	Security of network services	Yes	Yes				✓	✓
	A13.1.3	Segregation in networks	Yes	Yes				✓	✓
	A13.2	Information transfer							
	A13.2.1	Information transfer policies and procedures	Yes	Yes			✓	✓	✓
	A13.2.2	Agreements on information transfer	Yes	Yes			✓		✓
	A13.2.3	Electronic messaging	Yes	Yes				✓	✓
	A13.2.4	Confidentiality or non-disclosure agreements	Yes	Yes				✓	✓
A14 System acquisition, development and maintenance	A14.1	Security requirements of information systems							
	A14.1.1	Information security requirements analysis and specification	Yes	Yes				✓	✓
	A14.1.2	Securing applications services on public networks	Yes	Yes				✓	✓
	A14.1.3	Protecting application services transactions	Yes	Yes				✓	✓
	A14.2	Security in development and support processes							
	A14.2.1	Secure development policy	Yes	Yes			✓	✓	✓
	A14.2.2	System change control procedures	Yes	Yes				✓	✓
	A14.2.3	Technical review of applications after operating platform changes	Yes	Yes				✓	✓
	A14.2.4	Restrictions on changes to software packages	Yes	Yes				✓	✓
	A14.2.5	Secure system engineering principles	Yes	Yes			✓	✓	✓
	A14.2.6	Secure development environment	Yes	Yes				✓	✓
	A14.2.7	Outsourced development	No	N/A	Cirrus does not outsource. Any development is directly managed by Cirrus.				
	A14.2.8	System security testing	Yes	Yes				✓	✓
	A14.2.9	System acceptance testing	Yes	Yes				✓	✓
	A14.3	Test data							
	A14.3.1	Protection of test data	Yes	Yes		✓	✓	✓	✓
A15 Supplier relationships	A15.1	Information security in supplier relationships							
	A15.1.1	Information security policy for supplier relationships	Yes	Yes		✓	✓	✓	✓
	A15.1.1	Addressing security within supplier agreements	Yes	Yes		✓	✓	✓	✓
	A15.1.2	Information and communication technology supply chain	Yes	Yes				✓	✓
	A15.2	Supplier service delivery management							
	A15.2.1	Monitoring and review of supplier services	Yes	Yes				✓	✓
	A15.2.2	Managing changes to supplier services	Yes	Yes				✓	✓
A16 Information security incident management	A16.1	Management of information security incidents and improvements							
	A16.1.1	Responsibilities and procedures	Yes	Yes				✓	✓
	A16.1.2	Reporting information security events	Yes	Yes				✓	✓
	A16.1.3	Reporting information security weaknesses	Yes	Yes			✓	✓	✓
	A16.1.4	Assessment of and decision on information security events	Yes	Yes				✓	✓
	A16.1.5	Response to information security incidents	Yes	Yes		✓	✓	✓	✓
	A16.1.6	Learning from information security incidents	Yes	Yes				✓	✓
	A16.1.7	Collection of evidence	Yes	Yes				✓	✓

Statement of Applicability: Cirrus B.V.

Version: 1.2, *current as of 18-05-2022* Classification : Public

Legend (for Selected Controls and Reasons for controls selection) Source: Cirrus_Security_Framework_And_SOA_2013

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 Annex A controls			Applicable	Implemented	Reasson for exclusion	Selected Controls and Reasons for Selection			
Clause	Sec	Control Objective/Control				LR	CO	BR/BP	RRA
A17 Information security aspects of business continuity management	A17.1	Information security continuity							
	A17.1.1	Planning information security continuity	Yes	Yes			✓	✓	✓
	A17.1.2	Implementing information security continuity	Yes	Yes				✓	✓
	A17.1.3	Verify, review and evaluate information security continuity	Yes	Yes				✓	✓
	A17.2	Redundancies							
	A17.2.1	Availability of information processing facilities	Yes	Yes			✓	✓	✓
A18 Compliance	A18.1	Compliance with legal and contractual requirements							
	A18.1.1	Identification of applicable legislation and contractual requirements	Yes	Yes		✓			✓
	A18.1.2	Intellectual property rights	Yes	Yes		✓		✓	✓
	A18.1.3	Protection of records	Yes	Yes		✓			✓
	A18.1.4	Privacy and protection of personally identifiable information	Yes	Yes		✓			✓
	A18.1.5	Regulation of cryptographic controls	Yes	Yes		✓			✓
	A18.2	Information security reviews							
	A18.2.1	Independent review of information security	Yes	Yes				✓	✓
	A18.2.2	Compliance with security policies and standards	Yes	Yes				✓	✓
	A18.2.3	Technical compliance review	Yes	Yes				✓	✓