Aha!

Statement of Applicability

Legend (for Selected Controls and Reasons for controls selection)

LR: legal or regulatory requirements, **CO**: contractual obligations, **BR/BP**: business requirements/adopted best practices, **RRA**: results of risk assessment

Version Number: **4.0**

Current as of: **2024-04-19**

Reviewed and Approved by Aha! Management: **2024-04-19**

ISO/IEC 27001:2022 Annex A Controls			Applicable	Implemented	Justification for exclusion	Justification for Inclusion			
			Y/N	Full,partial,None,N/A		LR	CO	BR/BP	RRA
Clause	Sec	Control Objective/Control							
5 Organizational controls	5.1	Policies for information security	Yes	Full		X	X	X	X
	5.2	Information security roles and responsibilities	Yes	Full			X	X	X
	5.3	Segregation of duties	Yes	Full			X	X	X
	5.4	Management responsibilities	Yes	Full			X	X	
	5.5	Contact with authorities	Yes	Full		X	X	X	
	5.6	Contact with special interest groups	Yes	Full			X	X	X
	5.7	Threat intelligence	Yes	Full			X	X	X
	5.8	Information security in project management	Yes	Full			X	X	X
	5.9	Inventory of information and other associated assets	Yes	Full			X	X	X
	5.10	Acceptable use of information and other associated assets	Yes	Full			X	X	
	5.11	Return of assets	Yes	Full			X	X	
	5.12	Classification of information	Yes	Full		X	X	X	
	5.13	Labelling of information	Yes	Full			X	X	
	5.14	Information transfer	Yes	Full		X	X	X	
	5.15	Access control	Yes	Full		X	X	X	X
	5.16	Identity management	Yes	Full			X	X	
	5.17	Authentication information	Yes	Full			X	X	X
	5.18	Access rights	Yes	Full			X	X	X
	5.19	Information security policy in supplier relationships	Yes	Full		X	X	X	X
	5.20	Addressing information security within supplier agreements	Yes	Full		X	X	X	
	5.21	Managing information security in the ICT supply chain	Yes	Full		X	X	X	
	5.22	Monitoring, review and change management of supplier services	Yes	Full		X	X	X	X
	5.23	Information security for use of cloud services	Yes	Full			X	X	X
	5.24	Information security incident management planning and preparation	Yes	Full		X	X	X	
	5.25	Assessment and decision on information security events	Yes	Full		X	X	X	
	5.26	Response to information security incidents	Yes	Full		X	X	X	
	5.27	Learning from Information Security incidents	Yes	Full			X	X	
	5.28	Collection of evidence	Yes	Full		X	X	X	X
	5.29	Information security during disruption	Yes	Full		X		X	
	5.30	ICT readiness for business continuity	Yes	Full		X	X	X	X
	5.31	Legal, statutory, regulatory and contractual requirements	Yes	Full		X	X	X	X
	5.32	Intellectual property rights	Yes	Full			X	X	X
	5.33	Protection of records	Yes	Full			X	X	X
	5.34	Privacy and protection of PII	Yes	Full		X	X	X	X
	5.35	Independent review of information security	Yes	Full				X	X
	5.36	Compliance with policies, rules and standards for information security	Yes	Full		X	X	X	
	5.37	Documented operating procedures	Yes	Full				X	
6 People controls	6.1	Screening	Yes	Full			X	X	
	6.2	Terms and conditions of employment	Yes	Full			X	X	X
	6.3	Information Security awareness, education and training	Yes	Full		X	X	X	X
	6.4	Disciplinary process	Yes	Full			X	X	X
	6.5	Responsibilities after termination or change of employment	Yes	Full			X	X	
	6.6	Confidentiality or non-disclosure agreements	Yes	Full		X	X	X	X
	6.7	Remote working	Yes	Full			X	X	X
	6.8	Information security event reporting	Yes	Full			X	X	
7 Physical controls	7.1	Physical security perimeters	No	N/A	Aha! does not maintain any physical corporate office location or facility.				
	7.2	Physical entry	No	N/A	Aha! does not maintain any physical corporate office location or facility.				
	7.3	Securing offices, rooms and facilities	No	N/A	Aha! does not maintain any physical corporate office location or facility.				
	7.4	Physical security monitoring	No	N/A	Aha! does not maintain any physical corporate office location or facility.				
	7.5	Protecting against physical and environmental threats	No	N/A	Aha! does not maintain any physical corporate office location or facility.				
	7.6	Working in secure areas	No	N/A	Aha! does not maintain any physical corporate office location or facility.				
	7.7	Clear desk and clear screen	Yes	Full			X	X	X
	7.8	Equipment siting and protection	No	N/A	Aha! does not maintain any physical corporate office location or facility.				
	7.9	Security of assets off-premises	Yes	Full		X	X	X	X
	7.10	Storage media	Yes	Full		X	X	X	
	7.11	Supporting utilities	No	N/A	Aha! does not maintain any physical corporate office location or facility.				
	7.12	Cabling security	No	N/A	Aha! does not maintain any physical corporate office location or facility.				
	7.13	Equipment maintenance	No	N/A	Aha! does not maintain any physical corporate office location or facility.				
	7.14	Secure disposal or re-use of equipment	Yes	Full		X	X	X	
	8.1	User endpoint devices	Yes	Full			X	X	X
	8.2	Privileged access rights	Yes	Full		X	X	X	X
	8.3	Information access restriction	Yes	Full		X	X	X	X
	8.4	Access to source code	Yes	Full			X	X	X
	8.5	Secure authentication	Yes	Full			X	X	
	8.6	Capacity management	Yes	Full				X	
	8.7	Protection against malware	Yes	Full			X	X	X
	8.8	Management of technical vulnerabilities	Yes	Full		X	X	X	
	8.9	Configuration management	Yes	Full		X	X	X	X
	8.10	Information deletion	Yes	Full		X	X	X	X
	8.11	Data masking	Yes	Full		X	X	X	X
	8.12	Data leakage prevention	Yes	Full		X	X	X	X
	8.13	Information backup	Yes	Full		X	X	X	X

8 Technological controls	8.14	Redundancy of information processing facilities	Yes	Full				X	X
	8.15	Logging	Yes	Full			X	X	X
	8.16	Monitoring activities	Yes	Full			X	X	X
	8.17	Clock synchronization	Yes	Full				X	
	8.18	Use of privileged utility programs	Yes	Full			X	X	
	8.19	Installation of software on operational systems	Yes	Full				X	
	8.20	Networks security	Yes	Full		X	X	X	X
	8.21	Security of network services	Yes	Full		X	X	X	X
	8.22	Segregation of networks	Yes	Full				X	X
	8.23	Web filtering	Yes	Full			X	X	
	8.24	Use of cryptography	Yes	Full		X	X	X	
	8.25	Secure development life cycle	Yes	Full			X	X	X
	8.26	Application security requirements	Yes	Full		X	X	X	X
	8.27	Secure system architecture and engineering principles	Yes	Full		X	X	X	
	8.28	Secure coding	Yes	Full			X	X	X
	8.29	Security testing in development and acceptance	Yes	Full			X	X	X
	8.30	Outsourced development	No	N/A	Aha! does not outsource software development.				
	8.31	Separation of development, test and production environments	Yes	Full			X	X	
	8.32	Change management	Yes	Full			X	X	X
	8.33	Test information	Yes	Partial	No customer data from production systems is used for testing. The test data does NOT need to be protected.		X	X	
	8.34	Protection of information systems during audit testing	Yes	Full			X	X	X