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: **3.0**

Current as of: **2023-04-04**

Reviewed and Approved by Aha! Management: **2023-04-04**

ISO/IEC 27001:2013 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 Security Policies	5.1	Management direction for Information Security							
	5.1.1	Policies for Information Security	Yes	Full		X	X	X	X
	5.1.2	Review of the policies for Information Security	Yes	Full		X	X	X	
6 Organization of Information Security	6.1	Internal organization							
	6.1.1	Information Security roles and responsibilities	Yes	Full			X	X	X
	6.1.2	Segregation of duties	Yes	Full			X	X	X
	6.1.3	Contact with authorities	Yes	Full		X	X	X	
	6.1.4	Contact with special interest groups	Yes	Full			X	X	X
	6.1.5	Information Security in project management	Yes	Full			X	X	X
	6.2	Mobile devices and teleworking							
	6.2.1	Mobile device policy	Yes	Full		X	X	X	X
	6.2.2	Teleworking	Yes	Full			X	X	X
7 Human resource security	7.1	Prior to employment							
	7.1.1	Screening	Yes	Full			X	X	
	7.1.2	Terms and conditions of employment	Yes	Full			X	X	X
	7.2	During employment							
	7.2.1	Management responsibilities	Yes	Full			X	X	
	7.2.2	Information Security awareness, education and training	Yes	Full		X	X	X	X
	7.2.3	Disciplinary process	Yes	Full			X	X	X
	7.3	Termination and change of employment							
	7.3.1	Termination or change of employment responsibilities	Yes	Full			X	X	
8 Asset management	8.1	Responsibility for assets							
	8.1.1	Inventory of assets	Yes	Full			X	X	X
	8.1.2	Ownership of assets	Yes	Full			X	X	X
	8.1.3	Acceptable use of assets	Yes	Full			X	X	
	8.1.4	Return of assets	Yes	Full			X	X	
	8.2	Information classification							
	8.2.1	Classification of information	Yes	Full		X	X	X	
	8.2.2	Labeling of information	Yes	Full			X	X	
	8.2.3	Handling of assets	Yes	Full		X	X	X	X
	8.3	Media handling							
	8.3.1	Management of removable media	Yes	Full			X	X	
	8.3.2	Disposal of media	Yes	Full		X	X	X	
	8.3.3	Physical media transfer	Yes	Full			X	X	
9 Access control	9.1	Business requirements of access control							
	9.1.1	Access control policy	Yes	Full		X	X	X	X
	9.1.2	Access to networks and network services	Yes	Full		X	X	X	X
	9.2	User access management							
	9.2.1	User registration and de-registration	Yes	Full			X	X	
	9.2.2	User access provisioning	Yes	Full			X	X	
	9.2.3	Management of privileged access rights	Yes	Full		X	X	X	X
	9.2.4	Management of secret authentication information of users	Yes	Full			X	X	
	9.2.5	Review of user access rights	Yes	Full			X	X	X
	9.2.6	Removal or adjustment of access rights	Yes	Full			X	X	
	9.3	User responsibilities							
	9.3.1	Use of secret authentication information	Yes	Full			X	X	
	9.4	System and application access control							
	9.4.1	Information access restriction	Yes	Full		X	X	X	X
	9.4.2	Secure log-on procedures	Yes	Full			X	X	
	9.4.3	Password management system	Yes	Full			X	X	X
	9.4.4	Use of privileged utility programs	Yes	Full			X	X	
	9.4.5	Access control to program source code	Yes	Full			X	X	X
10 Cryptography	10.1	Cryptographic controls							
	10.1.1	Policy on the use of cryptographic controls	Yes	Full		X	X	X	
	10.1.2	Key management	Yes	Full			X	X	
11 Physical and environmental security	11.1	Secure areas							
	11.1.1	Physical security perimeter	No	N/A	Aha! does not maintain any physical corporate office location or facility.				
	11.1.2	Physical entry controls	No	N/A	Aha! does not maintain any physical corporate office location or facility.				
	11.1.3	Securing office, room and facilities	No	N/A	Aha! does not maintain any physical corporate office location or facility.				
	11.1.4	Protecting against external end environmental threats	No	N/A	Aha! does not maintain any physical corporate office location or facility.				
	11.1.5	Working in secure areas	No	N/A	Aha! does not maintain any physical corporate office location or facility.				
	11.1.6	Delivery and loading areas	No	N/A	Aha! does not maintain any physical corporate office location or facility.				
	11.2	Equipment							
	11.2.1	Equipment siting and protection	No	N/A	Aha! does not maintain any physical corporate office location or facility.				
	11.2.2	Supporting utilities	No	N/A	Aha! does not maintain any physical corporate office location or facility.				
	11.2.3	Cabling security	No	N/A	Aha! does not maintain any physical corporate office location or facility.				

	11.2.4	Equipment maintenance	No	N/A	Aha! does not maintain any physical corporate office location or facility.				
	11.2.5	Removal of assets	No	N/A	Aha! does not maintain any physical corporate office location or facility.				
	11.2.6	Security of equipment and assets off-premises	Yes	Full		X	X	X	X
	11.2.7	Secure disposal or re-use of equipment	Yes	Full		X	X	X	
	11.2.8	Unattended user equipment	Yes	Full			X	X	X
	11.2.9	Clear desk and clear screen policy	Yes	Full			X	X	X
12 Operations security	12.1	Operational procedures and responsibilities							
	12.1.1	Documented operating procedures	Yes	Full				X	
	12.1.2	Change management	Yes	Full			X	X	X
	12.1.3	Capacity management	Yes	Full				X	
	12.1.4	Separation of development, testing and operational environments	Yes	Full			X	X	
	12.2	Protection from malware							
	12.2.1	Controls against malware	Yes	Full			X	X	X
	12.3	Backup							
	12.3.1	Information backup	Yes	Full		X	X	X	
	12.4	Logging and monitoring							
	12.4.1	Event logging	Yes	Full			X	X	X
	12.4.2	Protection of log information	Yes	Full			X	X	
	12.4.3	Administrator and operator logs	Yes	Full				X	X
	12.4.4	Clock synchronization	Yes	Full				X	
	12.5	Control of operational software							
	12.5.1	Installation of software on operational systems	Yes	Full				X	
	12.6	Technical vulnerability management							
	12.6.1	Management of technical vulnerabilities	Yes	Full		X	X	X	
	12.6.2	Restrictions on software installation	Yes	Full				X	
	12.7	Information systems audit considerations							
	12.7.1	Information systems audit controls	Yes	Full			X	X	X
13 Communications security	13.1	Network security management				X	X	X	X
	13.1.1	Network controls	Yes	Full		X	X	X	X
	13.1.2	Security of network services	Yes	Full		X	X	X	X
	13.1.3	Segregation in networks	Yes	Full				X	X
	13.2	Information transfer							
	13.2.1	Information transfer policies and procedures	Yes	Full		X	X	X	
	13.2.2	Agreements on information transfer	No	N/A	Aha! does not transfer information to external parties for their own use. Supplier relationship agreements cover information security and privacy.				
	13.2.3	Electronic messaging	Yes	Full			X	X	
	13.2.4	Confidentiality or non-disclosure agreements	Yes	Full		X	X	X	X
14 System acquisition, development and maintenance	14.1	Security requirements of information systems							
	14.1.1	Information Security requirements analysis and specification	Yes	Full			X	X	X
	14.1.2	Securing applications services on public networks	Yes	Full		X	X	X	X
	14.1.3	Protecting application services transactions	Yes	Full		X	X	X	X
	14.2	Security in development and support processes							
	14.2.1	Secure development policy	Yes	Full			X	X	X
	14.2.2	System change control procedures	Yes	Full			X	X	
	14.2.3	Technical review of applications after operating platform changes	Yes	Full			X	X	X
	14.2.4	Restrictions on changes to software packages	Yes	Full			X	X	X
	14.2.5	Secure system engineering principles	Yes	Full		X	X	X	
	14.2.6	Secure development environment	Yes	Full			X	X	
	14.2.7	Outsourced development	No	N/A	Aha! does not outsource software development.				
	14.2.8	System security testing	Yes	Full			X	X	X
	14.2.9	System acceptance testing	Yes	Full			X	X	
	14.3	Test data							
	14.3.1	Protection of test data	Yes	Partial	No customer data from production systems is used for testing. The test data does NOT need to be protected.		X	X	
15 Supplier relationships	15.1	Information Security in supplier relationships							
	15.1.1	Information Security policy for supplier relationships	Yes	Full		X	X	X	X
	15.1.2	Addressing security within supplier agreements	Yes	Full		X	X	X	
	15.1.3	Information and communication technology supply chain	Yes	Full		X	X	X	
	15.2	Supplier service delivery management							
	15.2.1	Monitoring and review of supplier services	Yes	Full		X	X	X	X
	15.2.2	Managing changes to supplier services	Yes	Full			X	X	
16 Information Security incident management	16.1	Management of Information Security incidents and improvements							
	16.1.1	Responsibilities and procedures	Yes	Full		X	X	X	X
	16.1.2	Reporting Information Security events	Yes	Full			X	X	
	16.1.3	Reporting Information Security weaknesses	Yes	Full			X	X	
	16.1.4	Assessment of and decision on Information Security events	Yes	Full			X	X	
	16.1.5	Response to Information Security incidents	Yes	Full			X	X	
	16.1.6	Learning from Information Security incidents	Yes	Full			X	X	
	16.1.7	Collection of evidence	Yes	Full		X	X	X	X
17 Information Security aspects of business continuity management	17.1	Information Security continuity							
	17.1.1	Planning Information Security continuity	Yes	Full		X		X	
	17.1.2	Implementing Information Security continuity	Yes	Full				X	
	17.1.3	Verify, review and evaluate Information Security continuity	Yes	Full				X	X
	17.2	Redundancies							
	17.2.1	Availability of information processing facilities	Yes	Full				X	X
18 Compliance	18.1	Compliance with legal and contractual requirements							
	18.1.1	Identification of applicable legislation and contractual requirements	Yes	Full		X	X	X	X
	18.1.2	Intellectual property rights	Yes	Full			X	X	X
	18.1.3	Protection of records	Yes	Full			X	X	X
	18.1.4	Privacy and protection of personally identifiable information	Yes	Full		X	X	X	X
	18.1.5	Regulation of cryptographic controls	Yes	Full		X	X	X	
	18.2	Information Security reviews							
	18.2.1	Independent review of Information Security	Yes	Full				X	X
	18.2.2	Compliance with security policies and standards	Yes	Full		X	X	X	
	18.2.3	Technical compliance review	Yes	Full			X	X	