DocuSign Envelope ID: 357FF0DB-A629-403C-AF08-5677D1E4B34E

Downloaded at Tue 26 Aug 2025 16:00:12 GMT
Downloaded by stephan.pericbat@snyk.io

snyk

Snyk Statement of Applicability

Owner	Snyk CISO
Purpose	To provide a summary of the objectives and controls that Snyk has implemented to protect information and assets owned by or entrusted to Snyk Ltd. To provide detailed mapping of the measures and controls in place, supporting a framework of established processes which meet the requirements set out in the ISO 27001:2022 and ISO 27017:2015 Standards as well as detailing any justification for inclusions and exclusions.
Affected Parties	All Snyk employees and contracted workers
Definitions	ISMS: Information Security Management System Status:Implementation Status Reason code listed as follows: L = Legal or regulatory requirement, C = Contractual obligation/s, B = Business requirement or adopted best practice, R = Result of a risk assessment
Review and Maintenance	At a minimum, this document shall be reviewed annually or if a significant change to the Snyk ISMS occurs.
Version:	4
Date:	9th February 2024

Control ref:	Controls Description	Applicable	Status of impl	Reason Code				Location of supporting documentation
				L	C	B	R	
A.5.1	Policies for information security	Yes	Full			x		IS Compliance manual
A.5.2	Information security roles and responsibilities	Yes	Full			x		IS Compliance manual
A.5.3	Segregation of duties	Yes	Full			x		IS Compliance manual / Job Desciptions / Access Management
A.5.4	Management responsibilities	Yes	Full			x		IS Compliance manual / Job Descriptions
A.5.5	Contact with authorities	Yes	Full	x				IS Compliance manual
A.5.6	Contact with special interest groups	Yes	Full			x		IS Compliance manual
A.5.7	Threat intelligence	Yes	Full			x		Threat modelling standard, threat and detetion practices
A.5.8	Information security in project management	Yes	Full			x		Project management processes & operational processes
A.5.9	Inventory of information and other associated assets	Yes	Full			x		Asset Management
A.5.10	Acceptable use of information and other associated assets	Yes	Full			x		Employee AUP, Information classification and handling policy
A.5.11	Return of assets	Yes	Full			x		Employee AUP, Leavers process
A.5.12	Classification of Information	Yes	Full			x		Information Classifictation and handling policy
A.5.13	Labelling of information	Yes	Full			x		Information Classifictation and handling policy
A.5.14	Information transfer	Yes	Full			x		Information Classifictation and handling policy
A.5.15	Access control	Yes	Full			x		Access control policy
A.5.16	Identity management	Yes	Full			x		
A.5.17	Authentication information	Yes	Full			x		
A.5.18	Access rights	Yes	Full			x		
A.5.19	Information security in supplier relationships	Yes	Full		x	x		Procurement processes, Supplier ecurity review, Contracts and DPA's
A.5.20	Addressing information security within supplier agreements	Yes	Full		x	x		
A.5.21	Managing information security in the ICT supply chain	Yes	Full		x	x		
A.5.22	Monitoring, review and change management of supplier services	Yes	Full		x	x		
A.5.23	Information security for use of cloud services	Yes	Full		x	x		
A.5.24	Information security incident management planning and preparation	Yes	Full			x		

DocuSign Envelope ID: 357FF0DB-A629-403C-AF08-5677D1E4B34E

Downloaded at Tue, 26 Aug 2025 15:32:12 GMT
Downloaded by stephen.perciballi@snyk.io

A.5.25	Assessment and decision on information security events	Yes	Full			x		Incident Management Policy and post mortem process
A.5.26	Response to information security incidents	Yes	Full			x		
A.5.27	Learning from information security incidents	Yes	Full			x		
A.5.28	Collection of evidence	Yes	Full			x		
A.5.29	Information security during disruption	Yes	Partial			x		Shared with Cloud & SaaS Service providers, Snyks Business continuity and recovery policy
A.5.30	ICT readiness for business continuity	Yes	Partial			x		
A.5.31	Legal, statutory, regulatory and contractual requirements	Yes	Full	x	x	x		Legal register
A.5.32	Intellectual property rights	Yes	Full	x	x	x		Legal register and intellectual property policy
A.5.33	Protection of records	Yes	Full		x	x		Legal Register / internal & external privay policies
A.5.34	Privacy and protection of PII	Yes	Full	x	x	x		Legal Register / internal & external privay policies
A.5.35	Independent review of information security	Yes	Full		x	x		Information Security Management reviews, operational meetings, external audit, internal audit
A.5.36	Compliance with policies, rules and standards for information security	Yes	Full			x		
A.5.37	Documented operating procedures	Yes	Full			x		Snyk Intranet
A.6.1	Screening	Yes	Full	x	x	x		Background screening policy
A.6.2	Terms and conditions of employment	Yes	Full	x	x			Snyk employee and contractor terms
A.6.3	Information security awareness, education and training	Yes	Full		x	x		Security training and awareness program
A.6.4	Disciplinary process	Yes	Full	x	x	x		Snyk Disciplinary policy
A.6.5	Responsibilities after termination or change of employment	Yes	Full		x	x		Snyk employee and contractor terms
A.6.6	Confidentiality or non-disclosure agreements	Yes	Full	x	x	x		Employee and supplier contracts
A.6.7	Remote working	Yes	Full		x	x		Mobile Device manaement and laptop management policies
A.6.8	Information security event reporting	Yes	Full	x	x	x		Incident management policy and post mortem process
A.7.1	Physical security perimeters	Yes	Partial		x	x		Shared with Cloud and offie Providers Snyk control in Phyiscal & Environmental Security policy , Removeable media policy, Employee information security policy
A.7.2	Physical entry	Yes	Partial		x	x		
A.7.3	Securing offices, rooms and facilities	Yes	Partial			x		
A.7.4	Physical security monitoring	Yes	Partial		x	x		
A.7.5	Protecting against physical and environmental threats	Yes	Partial		x	x		
A.7.6	Working in secure areas	Yes	Partial		x	x		
A.7.7	Clear desk and clear screen	Yes	Partial			x		
A.7.8	Equipment siting and protection	Yes	Partial			x		
A.7.9	Security of assets off-premises	Yes	Partial			x		
A.7.10	Storage media	Yes	Partial			x		
A.7.11	Supporting utilities	Yes	Partial			x		
A.7.12	Cabling security	Yes	Partial			x		
A.7.13	Equipment maintenance	Yes	Partial	x		x		
A.7.14	Secure disposal or reuse of equipment	Yes	Partial		x	x		
A.8.1	User endpoint devices	Yes	Full		x	x		Mobiile device management policy,
A.8.2	Privileged access rights	Yes	Full		x	x		Access management Policy
A.8.3	Information access restriction	Yes	Full		x	x		
A.8.4	Access to source code	Yes	Full			x		
A.8.5	Secure authentication	Yes	Full		x	x		
A.8.6	Capacity management	Yes	Full		x	x		Management Reviews / Monitoring and provisioning systems
A.8.7	Protection against malware	Yes	Full		x	x		Mobile Device mangement, vulnerability mangement, monitoring practices, asset management policy
A.8.8	Management of technical vulnerabilities	Yes	Full		x	x		Vulnerabitiy Management policy and Information Security management reviews, external audits and assessments
A.8.9	Configuration management	Yes	Full		x	x		
A.8.10	Information deletion	Yes	Full		x	x		

DocuSign Envelope ID: 357FF0DB-A629-403C-AF08-5677D1E4B34E

Downloaded at Tue, 26 Aug 2025 15:32:12 GMT
Downloaded by stephen.percibalk@snyk.io

A.8.11	Data masking	Yes	Full		x	x		
A.8.12	Data leakage prevention	Yes	Full		x	x		
A.8.13	Information backup	Yes	Full		x	x		Backup policies and processes
A.8.14	Redundancy of information processing facilities	Yes	Partial		x	x		Shared with Cloud Service providers, Snyk Cryptography standard
A.8.15	Logging	Yes	Full		x	x		Logging and monitoring practices
A.8.16	Monitoring activities	Yes	Full		x	x		
A.8.17	Clock synchronization	Yes	Full			x		NTP Time Sources poilcy
A.8.18	Use of privileged utility programs	Yes	Full			x		Access Management policy
A.8.19	Installation of software on operational systems	Yes	Full			x		Logging and monitoring practices, ISMS policy
A.8.20	Networks security	Yes	Full			x		Access Management policy, network management processes and diagrams
A.8.21	Security of network services	Yes	Full		x	x		Supplier contractual agreements
A.8.22	Segregation of networks	Yes	Full			x		Access Management policy, network management processes and diagrams
A.8.23	Web filtering	Yes	Full			x		Employee AUP, Information security management policy
A.8.24	Use of cryptography	Yes	Partial			x		Shared with Cloud Service providers, Snyk Cryptography standard
A.8.25	Secure development life cycle	Yes	Full		x	x		Continuous integration processes, SDLC & Information security standards
A.8.26	Application security requirements	Yes	Full			x		Access control policy, Cryptography standard, SDLC and information security standards
A.8.27	Secure system architecture and engineering principles	Yes	Full			x		
A.8.28	Secure coding	Yes	Full			x		
A.8.29	Security testing in development and acceptance	Yes	Full			x		
A.8.30	Outsourced development	Yes	Full			x		
A.8.31	Separation of development, test and production environments	Yes	Full			x		
A.8.32	Change management	Yes	Full			x		
A.8.33	Test information	Yes	Full			x		
A.8.34	Protection of information systems during audit testing	Yes	Full			x		Audit and assessment process
Additional Cloud Controls ISO27017:2015								
CLD 6.3.1	Shared roles and responsibilities within a cloud computing environmentAssets of the cloud service customer that are on the cloud service provider's premises should be removed and returned if necessary, in a timely manner upon termination of the cloud service agreement	Yes	Full	x	x	x		Snyks Terms of service and MSA: https://snyk.io/policies/terms-of-service/
CLD 8.1.5	Removal of cloud service customer assets. Assets of the cloud service customer that are on the cloud service provider's premises should be removed and returned if necessary, in a timely manner upon termination of the cloud service agreement	Yes	Full	x	x	x		Asset Management
CLD 9.5.1	Segregation in virtual computing environments. A cloud service customer's virtual environment running on a cloud service should be protected from other cloud service customers and unauthorized persons.	Yes	Full		x	x		Network Management /Corporate and Infrastructure operation policies
CLD 9.5.2	Virtual machine hardening. Virtual machines in a cloud computing environment should be hardened to meet business needs.	Yes	Full		x	x		Corporate and Infrastructure operation policies
CLD 12.1.5	Administrator's operational security. Procedures for administrative operations of a cloud computing environment should be defined, documented, and monitored.	Yes	Full		x	x		Network Management /Corporate and Infrastructure operation policies
CLD 12.4.5	Monitoring of cloud services. The cloud service customer should have the capability to monitor specified aspects of the operation of the cloud services that the cloud service customer uses.	Yes	Full		x	x		Logging and Monitoring practises
CLD 13.1.4	Alignment of security management for virtual and physical networks. Upon configuration of virtual networks, consistency of configurations between virtual and physical networks should be verified based on the cloud service provider's network security policy.	Yes	Full		x	x		Network Management

DocuSigned by:
Myke Lyons
2B2D25DB1DD34D4...

March 4, 2024 | 6:10 PM EST

CISO

DocuSign Envelope ID: 357FF0DB-A629-403C-AF08-5677D1E4B34E

Downloaded at Tue, 26 Aug 2025 15:33:12 GMT
Downloaded by stephen.perciballi@snyk.io