rocket.chat Statement of Applicability | ISO 27001:2022 Annex A

Last reviewed: July, 2025

ISO 27001 Annex A Control	Title	Is this Applicable?
5	Organisational Controls	
5.1	Policies for information security	Applicable
5.2	Information security roles and responsibilities	Applicable
5.3	Segregation of duties	Applicable
5.4	Management Responsibilities	Applicable
5.5	Contact with Authorities	Applicable
5.6	Contact with special interest groups	Applicable
5.7	Threat intelligence	Applicable
5.8	Information security in project management	Applicable
5.9	Inventory of information and other associated assets	Applicable
5.10	Acceptable use of information and other associated assets	Applicable
5.11	Return of Assets	Applicable
5.12	Classification Of Information	Applicable
5.13	Labelling of Information	Applicable
5.14	Information Transfer	Applicable
5.15	Access Control	Applicable
5.16	Identity Management	Applicable
5.17	Authentication information	Applicable
5.18	Access rights	Applicable
5.19	Information security in supplier relationships	Applicable
5.20	Addressing information security within supplier agreements	Applicable
5.21	Managing information security in the ICT supply chain	Applicable
5.22	Monitoring, review and change management of supplier services	Applicable
5.23	Information security for use of cloud services	Applicable
5.24	Information security incident management planning and preparation	Applicable
5.25	Assessment and decision on information security events	Applicable
5.26	Response to information security incidents	Applicable
5.27	Learning from information security incidents	Applicable
5.28	Collection of evidence	Applicable
5.29	Information security during disruption	Applicable
5.30	ICT readiness for business continuity	Applicable
5.31	Legal, statutory, regulatory and contractual requirements	Applicable
5.32	Intellectual property rights	Applicable
5.33	Protection of records	Applicable
5.34	Privacy and protection of PII	Applicable
5.35	Independent review of information security	Applicable
5.36	Compliance with policies, rules and standards for information security	Applicable
5.37	Documented operating procedures	Applicable
6	People Controls	
6.1	Screening	Applicable
6.2	Terms and conditions of employment	Applicable
6.3	Information security awareness, education and training	Applicable
6.4	Disciplinary process	Applicable
6.5	Responsibilities after termination or change of employment	Applicable
6.6	Confidentiality or non-disclosure agreements	Applicable
6.7	Remote working	Applicable
6.8	Information security event reporting	Applicable
7	Physical Controls	
7.1	Physical security perimeters	Not Applicable
7.2	Physical entry	Not Applicable
7.3	Securing offices, rooms and facilities	Not Applicable

rocket.chat Statement of Applicability | ISO 27001:2022 Annex A

Last reviewed: July, 2025

ISO 27001 Annex A Control	Title	Is this Applicable?
7.4	Physical security monitoring	Not Applicable
7.5	Protecting against physical and environmental threats	Not Applicable
7.6	Working in secure areas	Not Applicable
7.7	Clear desk and clear screen	Applicable
7.8	Equipment siting and protection	Not Applicable
7.9	Security of assets off-premises	Applicable
7.10	Storage media	Applicable
7.11	Supporting utilities	Not Applicable
7.12	Cabling security	Not Applicable
7.13	Equipment maintenance	Not Applicable
7.14	Secure disposal or re-use of equipment	Applicable
8	Technological Controls	
8.1	User endpoint devices	Applicable
8.2	Privileged access rights	Applicable
8.3	Information access restriction	Applicable
8.4	Access to source code	Applicable
8.5	Secure authentication	Applicable
8.6	Capacity management	Applicable
8.7	Protection against malware	Applicable
8.8	Management of technical vulnerabilities	Applicable
8.9	Configuration management	Applicable
8.10	Information deletion	Applicable
8.11	Data masking	Not Applicable
8.12	Data leakage prevention	Applicable
8.13	Information backup	Applicable
8.14	Redundancy of information processing facilities	Applicable
8.15	Logging	Applicable
8.16	Monitoring activities	Applicable
8.17	Clock synchronization	Applicable
8.18	Use of privileged utility programs	Applicable
8.19	Installation of software on operational systems	Applicable
8.20	Networks security	Applicable
8.21	Security of network services	Applicable
8.22	Segregation of networks	Applicable
8.23	Web filtering	Not Applicable
8.24	Use of cryptography	Applicable
8.25	Secure development life cycle	Applicable
8.26	Application security requirements	Applicable
8.27	Secure system architecture and engineering principles	Applicable
8.28	Secure coding	Applicable
8.29	Security testing in development and acceptance	Applicable
8.30	Outsourced development	Not Applicable
8.31	Separation of development, test and production environments	Applicable
8.32	Change management	Applicable
8.33	Test information	Applicable
8.34	Protection of information systems during audit testing	Applicable