IC - ISO27001 - Statement of Applicabilty

Article Number: 357 | Rating: 5/5 from 1 votes | Last Updated: Wed, Mar 18, 2026 at 8:37 PM

Annex	Status	Reason
A 5.1 Policies for information security	Accepted	Risk Assessment
A 5.2 Information security roles and responsibilities	Accepted	Risk Assessment
A 5.3 Segregation of duties	Accepted	Risk Assessment
A 5.4 Management responsibilities	Accepted	Risk Assessment
A 5.5 Contact with authorities	Accepted	Risk Assessment
A 5.6 Contact with special interest groups	Accepted	Risk Assessment
A 5.7 Threat intelligence	Accepted	Risk Assessment
A 5.8 Information security in project management	Accepted	Risk Assessment
A 5.9 Inventory of information and other associated assets	Accepted	Risk Assessment
A 5.10 Acceptable use of information and other associated assets	Accepted	Risk Assessment
A 5.11 Return of assets	Accepted	Risk Assessment
A 5.12 Classification of information	Accepted	Risk Assessment
A 5.13 Labelling of information	Accepted	Risk Assessment
A 5.14 Information transfer	Accepted	Risk Assessment
A 5.15 Access control	Accepted	Risk Assessment
A 5.16 Identity management	Accepted	Risk Assessment
A 5.17 Authentication information	Accepted	Risk Assessment
A 5.18 Access rights	Accepted	Risk Assessment
A 5.19 Information security in supplier relationships	Accepted	Risk Assessment
A 5.20 Addressing information security within supplier agreements	Accepted	Risk Assessment
A 5.21 Managing information security in the ICT supply chain	Accepted	Risk Assessment
A 5.22 Monitoring, review and change management of supplier services	Accepted	Risk Assessment
A 5.23 Information security for use of cloud services	Accepted	Risk Assessment
A 5.24 Information security incident management planning and preparation	Accepted	Risk Assessment
A 5.25 Assessment and decision on information security events	Accepted	Risk Assessment
A 5.26 Response to information security incidents	Accepted	Risk Assessment
A 5.27 Learning from information security incidents	Accepted	Risk Assessment
A 5.28 Collection of evidence	Accepted	Risk Assessment
A 5.29 Information security during disruption	Accepted	Risk Assessment
A 5.30 ICT readiness for business continuity	Accepted	Risk Assessment
A 5.31 Identification of legal, statutory, regulatory and contractual requirements	Accepted	Risk Assessment
A 5.32 Intellectual property rights	Accepted	Risk Assessment
A 5.33 Protection of records	Accepted	Risk Assessment
A 5.34 Privacy and protection of PII	Accepted	Risk Assessment
A 5.35 Independent review of information security	Accepted	Risk Assessment
A 5.36 Compliance with policies and standards for information security	Accepted	Risk Assessment
A 5.37 Documented operating procedures	Accepted	Risk Assessment
A 6 People controls	Accepted	Risk Assessment
A 6.1 Screening	Accepted	Risk Assessment
A 6.2 Terms and conditions of employment	Accepted	Risk Assessment
A 6.3 Information security awareness, education and training	Accepted	Risk Assessment
A 6.4 Disciplinary process	Accepted	Risk Assessment
A 6.5 Responsibilities after termination or change of employment	Accepted	Risk Assessment
A 6.6 Confidentiality or non-disclosure agreements	Accepted	Risk Assessment
A 6.7 Remote working	Accepted	Risk Assessment
A 6.8 Information security event reporting	Accepted	Risk Assessment

A 7 Physical controls	Accepted	Risk Assessment
A 7.1 Physical security perimeter	Accepted	Risk Assessment
A 7.2 Physical entry controls	Accepted	Risk Assessment
A 7.3 Securing offices, rooms and facilities	Accepted	Risk Assessment
A 7.4 Physical security monitoring	Accepted	Risk Assessment
A 7.5 Protecting against physical and environmental threats	Accepted	Risk Assessment
A 7.6 Working in secure areas	Accepted	Risk Assessment
A 7.7 Clear desk and clear screen	Accepted	Risk Assessment
A 7.8 Equipment siting and protection	Accepted	Risk Assessment
A 7.9 Security of assets off-premises	Accepted	Risk Assessment
A 7.10 Storage media	Accepted	Risk Assessment
A 7.11 Supporting utilities	Accepted	Risk Assessment
A 7.12 Cabling security	Accepted	Risk Assessment
A 7.13 Equipment maintenance	Accepted	Risk Assessment
A 7.14 Secure disposal or re-use of equipment	Accepted	Risk Assessment
A 8 Technological controls	Accepted	Risk Assessment
A 8.1 User endpoint devices	Accepted	Risk Assessment
A 8.2 Privileged access rights	Accepted	Risk Assessment
A 8.3 Information access restriction	Accepted	Risk Assessment
A 8.4 Access to source code	Accepted	Risk Assessment
A 8.5 Secure authentication	Accepted	Risk Assessment
A 8.6 Capacity management	Accepted	Risk Assessment
A 8.7 Protection against malware	Accepted	Risk Assessment
A 8.8 Management of technical vulnerabilities	Accepted	Risk Assessment
A 8.9 Configuration management	Accepted	Risk Assessment
A 8.10 Information deletion	Accepted	Risk Assessment
A 8.11 Data masking	Accepted	Risk Assessment
A 8.12 Data leakage prevention	Accepted	Risk Assessment
A 8.13 Information backup	Accepted	Risk Assessment
A 8.14 Redundancy of information processing facilities	Accepted	Risk Assessment
A 8.15 Logging	Accepted	Risk Assessment
A 8.16 Monitoring activities	Accepted	Risk Assessment
A 8.17 Clock synchronisation	Accepted	Risk Assessment
A 8.18 Use of privileged utility programs	Accepted	Risk Assessment
A 8.19 Installation of software on operational systems	Accepted	Risk Assessment
A 8.20 Network controls	Accepted	Risk Assessment
A 8.21 Security of network services	Accepted	Risk Assessment
A 8.22 Segregation in networks	Accepted	Risk Assessment
A 8.23 Web filtering	Accepted	Risk Assessment
A 8.24 Use of cryptography	Accepted	Risk Assessment
A 8.25 Secure development lifecycle	Accepted	Risk Assessment
A 8.26 Application security requirements	Accepted	Risk Assessment
A 8.27 Secure system architecture and engineering principles	Accepted	Risk Assessment
A 8.29 Security testing in development and acceptance	Accepted	Risk Assessment
A 8.30 Outsourced development	Accepted	Risk Assessment
A 8.31 Separation of development, test and production environments	Accepted	Risk Assessment
A 8.32 Change management	Accepted	Risk Assessment
A 8.33 Test information	Accepted	Risk Assessment
A 8.34 Protection of information systems during audit and testing	Accepted	Risk Assessment

Posted by: Jonathan - Thu, Jun 3, 2021 at 11:43 AM. This article has been viewed 4140 times.

Online URL: https://kb.ic.uk/article/ic-iso27001-statement-of-applicabilty-357.html (https://kb.ic.uk/article/ic-iso27001-statement-of-applicabilty-357.html)