

# ISO/IEC 27002:2022-02 (E)

## Information security, cybersecurity and privacy protection - Information security controls

---

<b>Contents</b>		<b>Page</b>
<b>Foreword</b>		<b>vi</b>
<b>Introduction</b>		<b>vii</b>
<b>1</b>	<b>Scope</b>	<b>1</b>
<b>2</b>	<b>Normative references</b>	<b>1</b>
<b>3</b>	<b>Terms, definitions and abbreviated terms</b>	<b>1</b>
	3.1 Terms and definitions	1
	3.2 Abbreviated terms	6
<b>4</b>	<b>Structure of this document</b>	<b>7</b>
	4.1 Clauses	7
	4.2 Themes and attributes	8
	4.3 Control layout	9
<b>5</b>	<b>Organizational controls</b>	<b>9</b>
	5.1 Policies for information security	9
	5.2 Information security roles and responsibilities	11
	5.3 Segregation of duties	12
	5.4 Management responsibilities	13
	5.5 Contact with authorities	14
	5.6 Contact with special interest groups	15
	5.7 Threat intelligence	15
	5.8 Information security in project management	17
	5.9 Inventory of information and other associated assets	18
	5.10 Acceptable use of information and other associated assets	20
	5.11 Return of assets	21
	5.12 Classification of information	22
	5.13 Labelling of information	23
	5.14 Information transfer	24
	5.15 Access control	27
	5.16 Identity management	29
	5.17 Authentication information	30
	5.18 Access rights	32
	5.19 Information security in supplier relationships	33
	5.20 Addressing information security within supplier agreements	35
	5.21 Managing information security in the ICT supply chain	37
	5.22 Monitoring, review and change management of supplier services	39
	5.23 Information security for use of cloud services	41
	5.24 Information security incident management planning and preparation	43
	5.25 Assessment and decision on information security events	44
	5.26 Response to information security incidents	45
	5.27 Learning from information security incidents	46
	5.28 Collection of evidence	46
	5.29 Information security during disruption	48
	5.30 ICT readiness for business continuity	48
	5.31 Legal, statutory, regulatory and contractual requirements	50
	5.32 Intellectual property rights	51
	5.33 Protection of records	53
	5.34 Privacy and protection of PII	54
	5.35 Independent review of information security	55

5.36	Compliance with policies, rules and standards for information security .....	56
5.37	Documented operating procedures .....	57
<b>6</b>	<b>People controls</b> .....	<b>58</b>
6.1	Screening .....	58
6.2	Terms and conditions of employment .....	59
6.3	Information security awareness, education and training .....	60
6.4	Disciplinary process .....	62
6.5	Responsibilities after termination or change of employment .....	63
6.6	Confidentiality or non-disclosure agreements .....	63
6.7	Remote working .....	65
6.8	Information security event reporting .....	66
<b>7</b>	<b>Physical controls</b> .....	<b>67</b>
7.1	Physical security perimeters .....	67
7.2	Physical entry .....	68
7.3	Securing offices, rooms and facilities .....	70
7.4	Physical security monitoring .....	70
7.5	Protecting against physical and environmental threats .....	71
7.6	Working in secure areas .....	72
7.7	Clear desk and clear screen .....	73
7.8	Equipment siting and protection .....	74
7.9	Security of assets off-premises .....	75
7.10	Storage media .....	76
7.11	Supporting utilities .....	77
7.12	Cabling security .....	78
7.13	Equipment maintenance .....	79
7.14	Secure disposal or re-use of equipment .....	80
<b>8</b>	<b>Technological controls</b> .....	<b>81</b>
8.1	User endpoint devices .....	81
8.2	Privileged access rights .....	83
8.3	Information access restriction .....	84
8.4	Access to source code .....	86
8.5	Secure authentication .....	87
8.6	Capacity management .....	89
8.7	Protection against malware .....	90
8.8	Management of technical vulnerabilities .....	92
8.9	Configuration management .....	95
8.10	Information deletion .....	97
8.11	Data masking .....	98
8.12	Data leakage prevention .....	100
8.13	Information backup .....	101
8.14	Redundancy of information processing facilities .....	102
8.15	Logging .....	103
8.16	Monitoring activities .....	106
8.17	Clock synchronization .....	108
8.18	Use of privileged utility programs .....	109
8.19	Installation of software on operational systems .....	110
8.20	Networks security .....	111
8.21	Security of network services .....	112
8.22	Segregation of networks .....	113
8.23	Web filtering .....	114
8.24	Use of cryptography .....	115
8.25	Secure development life cycle .....	117
8.26	Application security requirements .....	118
8.27	Secure system architecture and engineering principles .....	120
8.28	Secure coding .....	122
8.29	Security testing in development and acceptance .....	124
8.30	Outsourced development .....	126
8.31	Separation of development, test and production environments .....	127
8.32	Change management .....	128
8.33	Test information .....	129
8.34	Protection of information systems during audit testing .....	130
<b>- 2 -</b>	<b>Annex A (informative) Using attributes</b> .....	<b>132</b>

<b>Annex B (informative) Correspondence of ISO/IEC 27002:2022 (this document) with ISO/IEC 27002:2013</b> .....	<b>143</b>
<b>Bibliography</b> .....	<b>150</b>