DIN EN ISO/IEC 27002:2024-01 (E)

Information security, cybersecurity and privacy protection - Information security controls (ISO/IEC 27002:2022)

Contents

Page

European foreword ... **5**

Foreword ... **6**

Introduction ... **7**

1 Scope ... **10**

2 Normative references ... **10**

3 Terms, definitions and abbreviated terms ... **10**
3.1 Terms and definitions ... 10
3.2 Abbreviated terms ... 15

4 Structure of this document ... **16**
4.1 Clauses ... 16
4.2 Themes and attributes ... 17
4.3 Control layout ... 18

5 Organizational controls ... **18**
5.1 Policies for information security ... 18
5.2 Information security roles and responsibilities ... 20
5.3 Segregation of duties ... 21
5.4 Management responsibilities ... 22
5.5 Contact with authorities ... 23
5.6 Contact with special interest groups ... 24
5.7 Threat intelligence ... 24
5.8 Information security in project management ... 26
5.9 Inventory of information and other associated assets ... 27
5.10 Acceptable use of information and other associated assets ... 29
5.11 Return of assets ... 30
5.12 Classification of information ... 31
5.13 Labelling of information ... 32
5.14 Information transfer ... 33
5.15 Access control ... 36
5.16 Identity management ... 38
5.17 Authentication information ... 39
5.18 Access rights ... 41
5.19 Information security in supplier relationships ... 42
5.20 Addressing information security within supplier agreements ... 44
5.21 Managing information security in the ICT supply chain ... 46
5.22 Monitoring, review and change management of supplier services ... 48
5.23 Information security for use of cloud services ... 50
5.24 Information security incident management planning and preparation ... 52
5.25 Assessment and decision on information security events ... 54
5.26 Response to information security incidents ... 54
5.27 Learning from information security incidents ... 55
5.28 Collection of evidence ... 56
5.29 Information security during disruption ... 57
5.30 ICT readiness for business continuity ... 57
5.31 Legal, statutory, regulatory and contractual requirements ... 59
5.32 Intellectual property rights ... 60
5.33 Protection of records ... 62
5.34 Privacy and protection of PII ... 63
5.35 Independent review of information security ... 64
5.36 Compliance with policies, rules and standards for information security ... 65
5.37 Documented operating procedures ... 66

6 People controls **67**
6.1 Screening 67
6.2 Terms and conditions of employment 68
6.3 Information security awareness, education and training 69
6.4 Disciplinary process 71
6.5 Responsibilities after termination or change of employment 72
6.6 Confidentiality or non-disclosure agreements 72
6.7 Remote working 74
6.8 Information security event reporting 75

7 Physical controls **76**
7.1 Physical security perimeters 76
7.2 Physical entry 77
7.3 Securing offices, rooms and facilities 79
7.4 Physical security monitoring 79
7.5 Protecting against physical and environmental threats 80
7.6 Working in secure areas 81
7.7 Clear desk and clear screen 82
7.8 Equipment siting and protection 83
7.9 Security of assets off-premises 84
7.10 Storage media 85
7.11 Supporting utilities 86
7.12 Cabling security 87
7.13 Equipment maintenance 88
7.14 Secure disposal or re-use of equipment 89

8 Technological controls **90**
8.1 User endpoint devices 90
8.2 Privileged access rights 92
8.3 Information access restriction 93
8.4 Access to source code 95
8.5 Secure authentication 96
8.6 Capacity management 98
8.7 Protection against malware 99
8.8 Management of technical vulnerabilities 101
8.9 Configuration management 104
8.10 Information deletion 106
8.11 Data masking 107
8.12 Data leakage prevention 109
8.13 Information backup 110
8.14 Redundancy of information processing facilities 111
8.15 Logging 112
8.16 Monitoring activities 115
8.17 Clock synchronization 117
8.18 Use of privileged utility programs 118
8.19 Installation of software on operational systems 119
8.20 Networks security 120
8.21 Security of network services 121
8.22 Segregation of networks 122
8.23 Web filtering 123
8.24 Use of cryptography 124
8.25 Secure development life cycle 126
8.26 Application security requirements 127
8.27 Secure system architecture and engineering principles 129
8.28 Secure coding 131
8.29 Security testing in development and acceptance 133
8.30 Outsourced development 135
8.31 Separation of development, test and production environments 136

8.32 Change management 137
8.33 Test information 138
8.34 Protection of information systems during audit testing 139

Annex A (informative) **Using attributes** **141**

Annex B (informative) **Correspondence of ISO/IEC 27002:2022 (this document) with ISO/IEC 27002:2013** **152**

Bibliography **159**