

DIN ISO/IEC 27002:2016-11 (E)

Information technology - Security techniques - Code of practice for information security controls (ISO/IEC 27002:2013 + Cor. 1:2014 + Cor. 2:2015)

Contents	Page
National foreword	4
National Annex NA (informative) Bibliography	5
0 Introduction	6
1 Scope	9
2 Normative references	9
3 Terms and definitions	9
4 Structure of this standard	9
4.1 Clauses	9
4.2 Control categories	9
5 Information security policies	10
5.1 Management direction for information security	10
6 Organization of information security	12
6.1 Internal organization	12
6.2 Mobile devices and teleworking	15
7 Human resource security	18
7.1 Prior to employment	18
7.2 During employment	20
7.3 Termination and change of employment	23
8 Asset management	23
8.1 Responsibility for assets	23
8.2 Information classification	26
8.3 Media handling	28
9 Access control	30
9.1 Business requirements of access control	30
9.2 User access management	33
9.3 User responsibilities	37
9.4 System and application access control	38
10 Cryptography	42
10.1 Cryptographic controls	42
11 Physical and environmental security	45
11.1 Secure areas	45
11.2 Equipment	49
12 Operations security	55
12.1 Operational procedures and responsibilities	55
12.2 Protection from malware	58
12.3 Backup	60
12.4 Logging and monitoring	61

12.5	Control of operational software	63
12.6	Technical vulnerability management	65
12.7	Information systems audit considerations	67
13	Communications security	67
13.1	Network security management	67
13.2	Information transfer	70
14	System acquisition, development and maintenance	74
14.1	Security requirements of information systems	74
14.2	Security in development and support processes	77
14.3	Test data	83
15	Supplier relationships	84
15.1	Information security in supplier relationships	84
15.2	Supplier service delivery management	88
16	Information security incident management	90
16.1	Management of information security incidents and improvements	90
17	Information security aspects of business continuity management	95
17.1	Information security continuity	95
17.2	Redundancies	97
18	Compliance	98
18.1	Compliance with legal and contractual requirements	98
18.2	Information security reviews	102
	Bibliography	105