

DIN EN ISO/IEC 27002:2017-06 (E)

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

Contents		Page
European foreword		6
Foreword		7
0	Introduction	8
1	Scope	10
2	Normative references	10
3	Terms and definitions	10
4	Structure of this standard	10
4.1	Clauses	10
4.2	Control categories	10
5	Information security policies	11
5.1	Management direction for information security	11
5.1.1	Policies for information security	11
5.1.2	Review of the policies for information security	12
6	Organization of information security	13
6.1	Internal organization	13
6.1.1	Information security roles and responsibilities	13
6.1.2	Segregation of duties	13
6.1.3	Contact with authorities	14
6.1.4	Contact with special interest groups	14
6.1.5	Information security in project management	15
6.2	Mobile devices and teleworking	15
6.2.1	Mobile device policy	15
6.2.2	Teleworking	16
7	Human resource security	18
7.1	Prior to employment	18
7.1.1	Screening	18
7.1.2	Terms and conditions of employment	18
7.2	During employment	19
7.2.1	Management responsibilities	19
7.2.2	Information security awareness, education and training	20
7.2.3	Disciplinary process	21
7.3	Termination and change of employment	22
7.3.1	Termination or change of employment responsibilities	22
8	Asset management	22
8.1	Responsibility for assets	22
8.1.1	Inventory of assets	22
8.1.2	Ownership of assets	23
8.1.3	Acceptable use of assets	23
8.1.4	Return of assets	24
8.2	Information classification	24
8.2.1	Classification of information	24

8.2.2	Labelling of information	25
8.2.3	Handling of assets	25
8.3	Media handling	26
8.3.1	Management of removable media	26
8.3.2	Disposal of media	27
8.3.3	Physical media transfer	27
9	Access control	28
9.1	Business requirements of access control	28
9.1.1	Access control policy	28
9.1.2	Access to networks and network services	29
9.2	User access management	30
9.2.1	User registration and de-registration	30
9.2.2	User access provisioning	30
9.2.3	Management of privileged access rights	31
9.2.4	Management of secret authentication information of users	31
9.2.5	Review of user access rights	32
9.2.6	Removal or adjustment of access rights	32
9.3	User responsibilities	33
9.3.1	Use of secret authentication information	33
9.4	System and application access control	34
9.4.1	Information access restriction	34
9.4.2	Secure log-on procedures	35
9.4.3	Password management system	35
9.4.4	Use of privileged utility programs	36
9.4.5	Access control to program source code	37
10	Cryptography	37
10.1	Cryptographic controls	37
10.1.1	Policy on the use of cryptographic controls	37
10.1.2	Key management	38
11	Physical and environmental security	39
11.1	Secure areas	39
11.1.1	Physical security perimeter	40
11.1.2	Physical entry controls	40
11.1.3	Securing offices, rooms and facilities	41
11.1.4	Protecting against external and environmental threats	41
11.1.5	Working in secure areas	42
11.1.6	Delivery and loading areas	42
11.2	Equipment	42
11.2.1	Equipment siting and protection	43
11.2.2	Supporting utilities	43
11.2.3	Cabling security	44
11.2.4	Equipment maintenance	44
11.2.5	Removal of assets	45
11.2.6	Security of equipment and assets off-premises	45
11.2.7	Secure disposal or re-use of equipment	46
11.2.8	Unattended user equipment	46
11.2.9	Clear desk and clear screen policy	47
12	Operations security	47
12.1	Operational procedures and responsibilities	47
12.1.1	Documented operating procedures	47
12.1.2	Change management	48
12.1.3	Capacity management	49
12.1.4	Separation of development, testing and operational environments	49
12.2	Protection from malware	50
12.2.1	Controls against malware	50
12.3	Backup	51
12.3.1	Information backup	51
12.4	Logging and monitoring	52

12.4.1	Event logging	52
12.4.2	Protection of log information	53
12.4.3	Administrator and operator logs	54
12.4.4	Clock synchronisation	54
12.5	Control of operational software	54
12.5.1	Installation of software on operational systems	54
12.6	Technical vulnerability management	55
12.6.1	Management of technical vulnerabilities	55
12.6.2	Restrictions on software installation	57
12.7	Information systems audit considerations	57
12.7.1	Information systems audit controls	57
13	Communications security	58
13.1	Network security management	58
13.1.1	Network controls	58
13.1.2	Security of network services	58
13.1.3	Segregation in networks	59
13.2	Information transfer	59
13.2.1	Information transfer policies and procedures	60
13.2.2	Agreements on information transfer	61
13.2.3	Electronic messaging	61
13.2.4	Confidentiality or non-disclosure agreements	62
14	System acquisition, development and maintenance	63
14.1	Security requirements of information systems	63
14.1.1	Information security requirements analysis and specification	63
14.1.2	Securing application services on public networks	64
14.1.3	Protecting application services transactions	65
14.2	Security in development and support processes	66
14.2.1	Secure development policy	66
14.2.2	System change control procedures	66
14.2.3	Technical review of applications after operating platform changes	67
14.2.4	Restrictions on changes to software packages	68
14.2.5	Secure system engineering principles	68
14.2.6	Secure development environment	69
14.2.7	Outsourced development	69
14.2.8	System security testing	70
14.2.9	System acceptance testing	70
14.3	Test data	71
14.3.1	Protection of test data	71
15	Supplier relationships	71
15.1	Information security in supplier relationships	71
15.1.1	Information security policy for supplier relationships	71
15.1.2	Addressing security within supplier agreements	72
15.1.3	Information and communication technology supply chain	74
15.2	Supplier service delivery management	75
15.2.1	Monitoring and review of supplier services	75
15.2.2	Managing changes to supplier services	75
16	Information security incident management	76
16.1	Management of information security incidents and improvements	76
16.1.1	Responsibilities and procedures	76
16.1.2	Reporting information security events	77
16.1.3	Reporting information security weaknesses	78
16.1.4	Assessment of and decision on information security events	78
16.1.5	Response to information security incidents	78
16.1.6	Learning from information security incidents	79
16.1.7	Collection of evidence	79
17	Information security aspects of business continuity management	80
17.1	Information security continuity	80

17.1.1	Planning information security continuity	80
17.1.2	Implementing information security continuity	81
17.1.3	Verify, review and evaluate information security continuity	82
17.2	Redundancies	82
17.2.1	Availability of information processing facilities	82
18	Compliance	83
18.1	Compliance with legal and contractual requirements	83
18.1.1	Identification of applicable legislation and contractual requirements	83
18.1.2	Intellectual property rights	83
18.1.3	Protection of records	84
18.1.4	Privacy and protection of personally identifiable information	85
18.1.5	Regulation of cryptographic controls	85
18.2	Information security reviews	86
18.2.1	Independent review of information security	86
18.2.2	Compliance with security policies and standards	86
18.2.3	Technical compliance review	87
	Bibliography	88