

# DIN ISO/IEC 27002:2008-09 (E)

## Information technology - Security techniques - Code of practice for information security management (ISO/IEC 27002:2005)

---

<b>Contents</b>		<b>Page</b>
National foreword .....		6
National Annex NA (informative) Bibliography .....		6
Introduction .....		7
0.1	What is information security? .....	7
0.2	Why information security is needed? .....	8
0.3	How to establish security requirements .....	8
0.4	Assessing security risks .....	8
0.5	Selecting controls .....	8
0.6	Information security starting point .....	8
0.7	Critical success factors .....	9
0.8	Developing your own guidelines .....	10
1	Scope .....	11
2	Terms and definitions .....	11
3	Structure of this standard .....	14
3.1	Clauses .....	14
3.2	Main security categories .....	14
4	Risk assessment and treatment .....	15
4.1	Assessing security risks .....	15
4.2	Treating security risks .....	15
5	Security policy .....	17
5.1	Information security policy .....	17
5.1.1	Information security policy document .....	17
5.1.2	Review of the information security policy .....	18
6	Organization of information security .....	19
6.1	Internal organization .....	19
6.1.1	Management commitment to information security .....	19
6.1.2	Information security co-ordination .....	20
6.1.3	Allocation of information security responsibilities .....	20
6.1.4	Authorization process for information processing facilities .....	21
6.1.5	Confidentiality agreements .....	21
6.1.6	Contact with authorities .....	22
6.1.7	Contact with special interest groups .....	22
6.1.8	Independent review of information security .....	23
6.2	External parties .....	24
6.2.1	Identification of risks related to external parties .....	24
6.2.2	Addressing security when dealing with customers .....	25
6.2.3	Addressing security in third party agreements .....	26
7	Asset management .....	29
7.1	Responsibility for assets .....	29
7.1.1	Inventory of assets .....	29
7.1.2	Ownership of assets .....	30

7.1.3	Acceptable use of assets .....	30
7.2	Information classification .....	31
7.2.1	Classification guidelines .....	31
7.2.2	Information labeling and handling .....	31
8	Human resources security .....	33
8.1	Prior to employment .....	33
8.1.1	Roles and responsibilities .....	33
8.1.2	Screening .....	33
8.1.3	Terms and conditions of employment .....	34
8.2	During employment .....	35
8.2.1	Management responsibilities .....	35
8.2.2	Information security awareness, education, and training .....	36
8.2.3	Disciplinary process .....	36
8.3	Termination or change of employment .....	37
8.3.1	Termination responsibilities .....	37
8.3.2	Return of assets .....	37
8.3.3	Removal of access rights .....	38
9	Physical and environmental security .....	39
9.1	Secure areas .....	39
9.1.1	Physical security perimeter .....	39
9.1.2	Physical entry controls .....	40
9.1.3	Securing offices, rooms, and facilities .....	40
9.1.4	Protecting against external and environmental threats .....	41
9.1.5	Working in secure areas .....	41
9.1.6	Public access, delivery, and loading areas .....	42
9.2	Equipment security .....	42
9.2.1	Equipment siting and protection .....	42
9.2.2	Supporting utilities .....	43
9.2.3	Cabling security .....	44
9.2.4	Equipment maintenance .....	44
9.2.5	Security of equipment off-premises .....	45
9.2.6	Secure disposal or re-use of equipment .....	45
9.2.7	Removal of property .....	46
10	Communications and operations management .....	47
10.1	Operational procedures and responsibilities .....	47
10.1.1	Documented operating procedures .....	47
10.1.2	Change management .....	47
10.1.3	Segregation of duties .....	48
10.1.4	Separation of development, test, and operational facilities .....	48
10.2	Third party service delivery management .....	49
10.2.1	Service delivery .....	49
10.2.2	Monitoring and review of third party services .....	50
10.2.3	Managing changes to third party services .....	50
10.3	System planning and acceptance .....	51
10.3.1	Capacity management .....	51
10.3.2	System acceptance .....	51
10.4	Protection against malicious and mobile code .....	52
10.4.1	Controls against malicious code .....	52
10.4.2	Controls against mobile code .....	53
10.5	Back-up .....	54
10.5.1	Information back-up .....	54
10.6	Network security management .....	55
10.6.1	Network controls .....	55
10.6.2	Security of network services .....	56
10.7	Media handling .....	56
10.7.1	Management of removable media .....	56
10.7.2	Disposal of media .....	57
10.7.3	Information handling procedures .....	57
10.7.4	Security of system documentation .....	58

10.8	Exchange of information .....	58
10.8.1	Information exchange policies and procedures .....	59
10.8.2	Exchange agreements .....	60
10.8.3	Physical media in transit .....	61
10.8.4	Electronic messaging .....	62
10.8.5	Business information systems .....	62
10.9	Electronic commerce services .....	63
10.9.1	Electronic commerce .....	63
10.9.2	On-Line Transactions .....	64
10.9.3	Publicly available information .....	65
10.10	Monitoring .....	65
10.10.1	Audit logging .....	65
10.10.2	Monitoring system use .....	66
10.10.3	Protection of log information .....	67
10.10.4	Administrator and operator logs .....	68
10.10.5	Fault logging .....	68
10.10.6	Clock synchronization .....	68
11	Access control .....	70
11.1	Business requirements for access control .....	70
11.1.1	Access control policy .....	70
11.2	User access management .....	71
11.2.1	User registration .....	71
11.2.2	Privilege management .....	72
11.2.3	User password management .....	72
11.2.4	Review of user access rights .....	73
11.3	User responsibilities .....	73
11.3.1	Password use .....	74
11.3.2	Unattended user equipment .....	74
11.3.3	Clear desk and clear screen policy .....	75
11.4	Network access control .....	75
11.4.1	Policy on use of network services .....	76
11.4.2	User authentication for external connections .....	76
11.4.3	Equipment identification in networks .....	77
11.4.4	Remote diagnostic and configuration port protection .....	77
11.4.5	Segregation in networks .....	78
11.4.6	Network connection control .....	78
11.4.7	Network routing control .....	79
11.5	Operating system access control .....	79
11.5.1	Secure log-on procedures .....	79
11.5.2	User identification and authentication .....	80
11.5.3	Password management system .....	81
11.5.4	Use of system utilities .....	82
11.5.5	Session time-out .....	82
11.5.6	Limitation of connection time .....	82
11.6	Application and information access control .....	83
11.6.1	Information access restriction .....	83
11.6.2	Sensitive system isolation .....	84
11.7	Mobile computing and teleworking .....	84
11.7.1	Mobile computing and communications .....	84
11.7.2	Teleworking .....	85
12	Information systems acquisition, development and maintenance .....	87
12.1	Security requirements of information systems .....	87
12.1.1	Security requirements analysis and specification .....	87
12.2	Correct processing in applications .....	88
12.2.1	Input data validation .....	88
12.2.2	Control of internal processing .....	88
12.2.3	Message integrity .....	89
12.2.4	Output data validation .....	89
12.3	Cryptographic controls .....	90
12.3.1	Policy on the use of cryptographic controls .....	90

12.3.2	Key management .....	91
12.4	Security of system files .....	93
12.4.1	Control of operational software .....	93
12.4.2	Protection of system test data .....	94
12.4.3	Access control to program source code .....	94
12.5	Security in development and support processes .....	95
12.5.1	Change control procedures .....	95
12.5.2	Technical review of applications after operating system changes .....	96
12.5.3	Restrictions on changes to software packages .....	96
12.5.4	Information leakage .....	97
12.5.5	Outsourced software development .....	97
12.6	Technical Vulnerability Management .....	98
12.6.1	Control of technical vulnerabilities .....	98
13	Information security incident management .....	100
13.1	Reporting information security events and weaknesses .....	100
13.1.1	Reporting information security events .....	100
13.1.2	Reporting security weaknesses .....	101
13.2	Management of information security incidents and improvements .....	101
13.2.1	Responsibilities and procedures .....	102
13.2.2	Learning from information security incidents .....	103
13.2.3	Collection of evidence .....	103
14	Business continuity management .....	105
14.1	Information security aspects of business continuity management .....	105
14.1.1	Including information security in the business continuity management process .....	105
14.1.2	Business continuity and risk assessment .....	106
14.1.3	Developing and implementing continuity plans including information security .....	106
14.1.4	Business continuity planning framework .....	107
14.1.5	Testing, maintaining and re-assessing business continuity plans .....	108
15	Compliance .....	110
15.1	Compliance with legal requirements .....	110
15.1.1	Identification of applicable legislation .....	110
15.1.2	Intellectual property rights (IPR) .....	110
15.1.3	Protection of organizational records .....	111
15.1.4	Data protection and privacy of personal information .....	112
15.1.5	Prevention of misuse of information processing facilities .....	112
15.1.6	Regulation of cryptographic controls .....	113
15.2	Compliance with security policies and standards, and technical compliance .....	113
15.2.1	Compliance with security policies and standards .....	114
15.2.2	Technical compliance checking .....	114
15.3	Information systems audit considerations .....	115
15.3.1	Information systems audit controls .....	115
15.3.2	Protection of information systems audit tools .....	115
	Bibliography .....	117
	Index .....	118