

ISO/IEC 27002:2005-06 (E)

Information technology - Security techniques - Code of practice for information security management

Contents		Page
FOREWORD		VII
0	INTRODUCTION	VIII
0.1	WHAT IS INFORMATION SECURITY?	VIII
0.2	WHY INFORMATION SECURITY IS NEEDED?	VIII
0.3	HOW TO ESTABLISH SECURITY REQUIREMENTS	IX
0.4	ASSESSING SECURITY RISKS	IX
0.5	SELECTING CONTROLS	IX
0.6	INFORMATION SECURITY STARTING POINT	IX
0.7	CRITICAL SUCCESS FACTORS	X
0.8	DEVELOPING YOUR OWN GUIDELINES	XI
1	SCOPE	1
2	TERMS AND DEFINITIONS	1
3	STRUCTURE OF THIS STANDARD	4
3.1	CLAUSES	4
3.2	MAIN SECURITY CATEGORIES	4
4	RISK ASSESSMENT AND TREATMENT	5
4.1	ASSESSING SECURITY RISKS	5
4.2	TREATING SECURITY RISKS	5
5	SECURITY POLICY	7
5.1	INFORMATION SECURITY POLICY	7
5.1.1	Information security policy document	7
5.1.2	Review of the information security policy	8
6	ORGANIZATION OF INFORMATION SECURITY	9
6.1	INTERNAL ORGANIZATION	9
6.1.1	Management commitment to information security	9
6.1.2	Information security co-ordination	10
6.1.3	Allocation of information security responsibilities	10
6.1.4	Authorization process for information processing facilities	11
6.1.5	Confidentiality agreements	11
6.1.6	Contact with authorities	12
6.1.7	Contact with special interest groups	12
6.1.8	Independent review of information security	13
6.2	EXTERNAL PARTIES	14
6.2.1	Identification of risks related to external parties	14
6.2.2	Addressing security when dealing with customers	15
6.2.3	Addressing security in third party agreements	16
7	ASSET MANAGEMENT	19
7.1	RESPONSIBILITY FOR ASSETS	19
7.1.1	Inventory of assets	19
7.1.2	Ownership of assets	20
7.1.3	Acceptable use of assets	20
7.2	INFORMATION CLASSIFICATION	21
7.2.1	Classification guidelines	21

7.2.2	Information labeling and handling	21
8	HUMAN RESOURCES SECURITY	23
8.1	PRIOR TO EMPLOYMENT	23
8.1.1	Roles and responsibilities	23
8.1.2	Screening	23
8.1.3	Terms and conditions of employment	24
8.2	DURING EMPLOYMENT	25
8.2.1	Management responsibilities	25
8.2.2	Information security awareness, education, and training	26
8.2.3	Disciplinary process	26
8.3	TERMINATION OR CHANGE OF EMPLOYMENT	27
8.3.1	Termination responsibilities	27
8.3.2	Return of assets	27
8.3.3	Removal of access rights	28
9	PHYSICAL AND ENVIRONMENTAL SECURITY	29
9.1	SECURE AREAS	29
9.1.1	Physical security perimeter	29
9.1.2	Physical entry controls	30
9.1.3	Securing offices, rooms, and facilities	30
9.1.4	Protecting against external and environmental threats	31
9.1.5	Working in secure areas	31
9.1.6	Public access, delivery, and loading areas	32
9.2	EQUIPMENT SECURITY	32
9.2.1	Equipment siting and protection	32
9.2.2	Supporting utilities	33
9.2.3	Cabling security	34
9.2.4	Equipment maintenance	34
9.2.5	Security of equipment off-premises	35
9.2.6	Secure disposal or re-use of equipment	35
9.2.7	Removal of property	36
10	COMMUNICATIONS AND OPERATIONS MANAGEMENT	37
10.1	OPERATIONAL PROCEDURES AND RESPONSIBILITIES	37
10.1.1	Documented operating procedures	37
10.1.2	Change management	37
10.1.3	Segregation of duties	38
10.1.4	Separation of development, test, and operational facilities	38
10.2	THIRD PARTY SERVICE DELIVERY MANAGEMENT	39
10.2.1	Service delivery	39
10.2.2	Monitoring and review of third party services	40
10.2.3	Managing changes to third party services	40
10.3	SYSTEM PLANNING AND ACCEPTANCE	41
10.3.1	Capacity management	41
10.3.2	System acceptance	41
10.4	PROTECTION AGAINST MALICIOUS AND MOBILE CODE	42
10.4.1	Controls against malicious code	42
10.4.2	Controls against mobile code	43
10.5	BACK-UP	44
10.5.1	Information back-up	44
10.6	NETWORK SECURITY MANAGEMENT	45
10.6.1	Network controls	45
10.6.2	Security of network services	46
10.7	MEDIA HANDLING	46
10.7.1	Management of removable media	46
10.7.2	Disposal of media	47
10.7.3	Information handling procedures	47
10.7.4	Security of system documentation	48
10.8	EXCHANGE OF INFORMATION	48
10.8.1	Information exchange policies and procedures	49
10.8.2	Exchange agreements	50

10.8.3	Physical media in transit	51
10.8.4	Electronic messaging	52
10.8.5	Business information systems	52
10.9	ELECTRONIC COMMERCE SERVICES	53
10.9.1	Electronic commerce	53
10.9.2	On-Line Transactions	54
10.9.3	Publicly available information	55
10.10	MONITORING	55
10.10.1	Audit logging	55
10.10.2	Monitoring system use	56
10.10.3	Protection of log information	57
10.10.4	Administrator and operator logs	58
10.10.5	Fault logging	58
10.10.6	Clock synchronization	58
11	ACCESS CONTROL	60
11.1	BUSINESS REQUIREMENT FOR ACCESS CONTROL	60
11.1.1	Access control policy	60
11.2	USER ACCESS MANAGEMENT	61
11.2.1	User registration	61
11.2.2	Privilege management	62
11.2.3	User password management	62
11.2.4	Review of user access rights	63
11.3	USER RESPONSIBILITIES	63
11.3.1	Password use	64
11.3.2	Unattended user equipment	64
11.3.3	Clear desk and clear screen policy	65
11.4	NETWORK ACCESS CONTROL	65
11.4.1	Policy on use of network services	66
11.4.2	User authentication for external connections	66
11.4.3	Equipment identification in networks	67
11.4.4	Remote diagnostic and configuration port protection	67
11.4.5	Segregation in networks	68
11.4.6	Network connection control	68
11.4.7	Network routing control	69
11.5	OPERATING SYSTEM ACCESS CONTROL	69
11.5.1	Secure log-on procedures	69
11.5.2	User identification and authentication	70
11.5.3	Password management system	71
11.5.4	Use of system utilities	72
11.5.5	Session time-out	72
11.5.6	Limitation of connection time	72
11.6	APPLICATION AND INFORMATION ACCESS CONTROL	73
11.6.1	Information access restriction	73
11.6.2	Sensitive system isolation	74
11.7	MOBILE COMPUTING AND TELEWORKING	74
11.7.1	Mobile computing and communications	74
11.7.2	Teleworking	75
12	INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE	77
12.1	SECURITY REQUIREMENTS OF INFORMATION SYSTEMS	77
12.1.1	Security requirements analysis and specification	77
12.2	CORRECT PROCESSING IN APPLICATIONS	78
12.2.1	Input data validation	78
12.2.2	Control of internal processing	78
12.2.3	Message integrity	79
12.2.4	Output data validation	79
12.3	CRYPTOGRAPHIC CONTROLS	80
12.3.1	Policy on the use of cryptographic controls	80
12.3.2	Key management	81
12.4	SECURITY OF SYSTEM FILES	83
12.4.1	Control of operational software	83

12.4.2	Protection of system test data	84
12.4.3	Access control to program source code	84
12.5	SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES	85
12.5.1	Change control procedures	85
12.5.2	Technical review of applications after operating system changes	86
12.5.3	Restrictions on changes to software packages	86
12.5.4	Information leakage	87
12.5.5	Outsourced software development	87
12.6	TECHNICAL VULNERABILITY MANAGEMENT	88
12.6.1	Control of technical vulnerabilities	88
13	INFORMATION SECURITY INCIDENT MANAGEMENT	90
13.1	REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES	90
13.1.1	Reporting information security events	90
13.1.2	Reporting security weaknesses	91
13.2	MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS	91
13.2.1	Responsibilities and procedures	92
13.2.2	Learning from information security incidents	93
13.2.3	Collection of evidence	93
14	BUSINESS CONTINUITY MANAGEMENT	95
14.1	INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT	95
14.1.1	Including information security in the business continuity management process	95
14.1.2	Business continuity and risk assessment	96
14.1.3	Developing and implementing continuity plans including information security	96
14.1.4	Business continuity planning framework	97
14.1.5	Testing, maintaining and re-assessing business continuity plans	98
15	COMPLIANCE	100
15.1	COMPLIANCE WITH LEGAL REQUIREMENTS	100
15.1.1	Identification of applicable legislation	100
15.1.2	Intellectual property rights (IPR)	100
15.1.3	Protection of organizational records	101
15.1.4	Data protection and privacy of personal information	102
15.1.5	Prevention of misuse of information processing facilities	102
15.1.6	Regulation of cryptographic controls	103
15.2	COMPLIANCE WITH SECURITY POLICIES AND STANDARDS, AND TECHNICAL COMPLIANCE	103
15.2.1	Compliance with security policies and standards	104
15.2.2	Technical compliance checking	104
15.3	INFORMATION SYSTEMS AUDIT CONSIDERATIONS	105
15.3.1	Information systems audit controls	105
15.3.2	Protection of information systems audit tools	105
	BIBLIOGRAPHY	107
	INDEX	108