

ISO/IEC 27010:2012-04 (E)

Information technology - Security techniques - Information security management for inter-sector and inter-organizational communications

Contents		Page
Foreword		vi
Introduction		vii
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Concepts and justification	2
4.1	Introduction	2
4.2	Information sharing communities	2
4.3	Community management	2
4.4	Supporting entities	2
4.5	Inter-sector communication	2
4.6	Conformity	3
4.7	Communications model	4
5	Security policy	5
5.1	Information security policy	5
5.1.1	Information security policy document	5
5.1.2	Review of the information security policy	5
6	Organization of information security	5
6.1	Internal organization	5
6.2	External parties	5
6.2.1	Identification of risks related to external parties	5
6.2.2	Addressing security when dealing with customers	5
6.2.3	Addressing security in third party agreements	5
7	Asset management	6
7.1	Responsibility for assets	6
7.1.1	Inventory of assets	6
7.1.2	Ownership of assets	6
7.1.3	Acceptable use of assets	6
7.2	Information classification	6
7.2.1	Classification guidelines	6
7.2.2	Information labelling and handling	6
7.3	Information exchanges protection	7
7.3.1	Information dissemination	7
7.3.2	Information disclaimers	7
7.3.3	Information credibility	8
7.3.4	Information sensitivity reduction	8
7.3.5	Anonymous source protection	8
7.3.6	Anonymous recipient protection	9
7.3.7	Onwards release authority	9
8	Human resources security	9
8.1	Prior to employment	9
8.1.1	Roles and responsibilities	9

8.1.2	Screening	9
8.1.3	Terms and conditions of employment	9
8.2	During employment	10
8.3	Termination or change of employment	10
9	Physical and environmental security	10
10	Communications and operations management	10
10.1	Operational procedures and responsibilities	10
10.2	Third party service delivery management	10
10.3	System planning and acceptance	10
10.4	Protection against malicious and mobile code	10
10.4.1	Controls against malicious code	10
10.4.2	Controls against mobile code	10
10.5	Back-up	10
10.6	Network security management	11
10.7	Media handling	11
10.8	Exchange of information	11
10.8.1	Information exchange policies and procedures	11
10.8.2	Exchange agreements	11
10.8.3	Physical media in transit	11
10.8.4	Electronic messaging	11
10.8.5	Business information systems	11
10.9	Electronic commerce services	11
10.10	Monitoring	11
10.10.1	Audit logging	11
10.10.2	Monitoring system use	12
10.10.3	Protection of log information	12
10.10.4	Administrator and operator logs	12
10.10.5	Fault logging	12
10.10.6	Clock synchronisation	12
11	Access control	12
12	Information systems acquisition, development and maintenance	12
12.1	Security requirements of information systems	12
12.2	Correct processing in applications	12
12.3	Cryptographic controls	12
12.3.1	Policy on the use of cryptographic controls	12
12.3.2	Key management	12
12.4	Security of system files	13
12.5	Security in development and support processes	13
12.6	Technical vulnerability management	13
13	Information security incident management	13
13.1	Reporting information security events and weaknesses	13
13.1.1	Reporting information security events	13
13.1.2	Reporting security weaknesses	13
13.1.3	Early warning system	13
13.2	Management of information security incidents and improvements	14
13.2.1	Responsibilities and procedures	14
13.2.2	Learning from information security incidents	14
13.2.3	Collection of evidence	14
14	Business continuity management	14
14.1	Information security aspects of business continuity management	14
14.1.1	Including information security in the business continuity management process	14
14.1.2	Business continuity and risk assessment	14
14.1.3	Developing and implementing continuity plans including information security	14
14.1.4	Business continuity planning framework	15
14.1.5	Testing, maintaining and re-assessing business continuity plans	15

15	Compliance	15
15.1	Compliance with legal requirements	15
15.1.1	Identification of applicable legislation	15
15.1.2	Intellectual property rights (IPR)	15
15.1.3	Protection of organizational records	15
15.1.4	Data protection and privacy of personal information	15
15.1.5	Prevention of misuse of information processing facilities	15
15.1.6	Regulation of cryptographic controls	15
15.1.7	Liability to the information sharing community	15
15.2	Compliance with security policies and standards, and technical compliance	16
15.3	Information systems audit considerations	16
15.3.1	Information systems audit controls	16
15.3.2	Protection of information systems audit tools	16
15.3.3	Audit of community functions	16
Annex A (informative) Sharing sensitive information		17
Annex B (informative) Establishing trust in information exchanges		22
Annex C (informative) The Traffic Light Protocol		27
Annex D (informative) Models for organizing an information sharing community		28
Bibliography		34