

ISO/IEC 27011:2016-12 (E)

Information technology - Security techniques - Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations

Contents		Page
1	Scope	1
2	Normative references.....	1
3	Definitions and abbreviations	1
3.1	Definitions.....	1
3.2	Abbreviations	2
4	Overview	2
4.1	Structure of this Recommendation International Standard.....	2
4.2	Information security management systems in telecommunications organizations.....	3
5	Information security policies	5
6	Organization of information security.....	5
6.1	Internal organization	5
6.2	Mobile devices and teleworking.....	6
7	Human resource security	6
7.1	Prior to employment.....	6
7.2	During employment	7
7.3	Termination or change of employment	7
8	Asset management.....	7
8.1	Responsibility for assets.....	7
8.2	Information classification.....	8
8.3	Media handling.....	8
9	Access control	8
9.1	Business requirement for access control	8
9.2	User access management.....	9
9.3	User responsibilities	9
9.4	System and application access control	9
10	Cryptography.....	9
11	Physical and environmental security	9
11.1	Secure areas.....	9
11.2	Equipment	10
12	Operations security.....	12
12.1	Operational procedures and responsibilities.....	12
12.2	Protection from malware.....	13
12.3	Backup	13
12.4	Logging and monitoring.....	13
12.5	Control of operational software.....	13
12.6	Technical vulnerability management	14
12.7	Information systems audit considerations	14
13	Communications security	14
13.1	Network security management.....	14
13.2	Information transfer.....	15
14	System acquisition, development and maintenance	16
14.1	Security requirements of information systems	16
14.2	Security in development and support processes	16
14.3	Test data	16

15	Supplier relationships	16
15.1	Information security in supplier relationships	16
15.2	Supplier service delivery management.....	17
16	Information security incident management	17
16.1	Management of information security incidents and improvements.....	17
17	Information security aspects of business continuity management.....	19
17.1	Information security continuity	19
17.2	Redundancies	20
18	Compliance.....	20
	Annex A – Telecommunications extended control set	21
	Annex B – Additional guidance for network security	29
	B.1 Security measures against network attacks	29
	B.2 Network security measures for network congestion.....	30
	Bibliography.....	31