

# ISO/IEC 27011:2008-12 (E)

## Information technology\_ - Security techniques\_ - Information security management guidelines for telecommunications organizations based on ISO/IEC\_27002

---

### CONTENTS

	<i>Page</i>
1 Scope .....	1
2 Normative references .....	1
3 Definitions and abbreviations.....	1
3.1 Definitions.....	1
3.2 Abbreviations.....	2
4 Overview .....	3
4.1 Structure of this guideline .....	3
4.2 Information security management systems in telecommunications business.....	3
5 Security policy.....	5
6 Organization of information security .....	5
6.1 Internal organization.....	5
6.2 External parties.....	7
7 Asset management.....	10
7.1 Responsibility for assets .....	10
7.2 Information classification .....	12
8 Human resources security.....	13
8.1 Prior to employment .....	13
8.2 During employment.....	15
8.3 Termination or change of employment .....	15
9 Physical and environmental security.....	15
9.1 Secure areas .....	15
9.2 Equipment security.....	17
10 Communications and operations management .....	19
10.1 Operational procedures and responsibilities .....	19
10.2 Third party service delivery management.....	21
10.3 System planning and acceptance .....	21
10.4 Protection against malicious and mobile code .....	22
10.5 Back-up .....	22
10.6 Network security management.....	22
10.7 Media handling.....	23
10.8 Exchange of information .....	23
10.9 Electronic commerce services.....	23
10.10 Monitoring.....	23
11 Access control .....	25
11.1 Business requirement for access control.....	25
11.2 User access management .....	26
11.3 User responsibilities .....	26
11.4 Network access control .....	26
11.5 Operating system access control.....	26
11.6 Application and information access control .....	26
11.7 Mobile computing and teleworking.....	26
12 Information systems acquisition, development and maintenance .....	26
12.1 Security requirements of information systems.....	26
12.2 Correct processing in applications .....	26

12.3	Cryptographic controls .....	26
12.4	Security of system files .....	26
12.5	Security in development and support processes .....	27
12.6	Technical vulnerability management .....	27
13	Information security incident management .....	28
13.1	Reporting information security events and weaknesses .....	28
13.2	Management of information security incidents and improvements .....	29
14	Business continuity management .....	31
14.1	Information security aspects of business continuity management .....	31
15	Compliance .....	33
Annex A	– Telecommunications extended control set.....	34
A.9	Physical and environmental security .....	34
A.10	Communications and operations management.....	37
A.11	Access control .....	39
A.15	Compliance.....	39
Annex B	– Additional implementation guidance .....	42
B.1	Network security measures against cyber attacks.....	42
B.2	Network security measures for network congestion.....	42
Bibliography	.....	44