

ISO/IEC 27017:2015-12 (E)

Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Contents		Page
1	Scope	1
2	Normative references.....	1
2.1	Identical Recommendations International Standards	1
2.2	Additional References	1
3	Definitions and abbreviations.....	1
3.1	Terms defined elsewhere.....	1
3.2	Abbreviations	2
4	Cloud sector-specific concepts	2
4.1	Overview	2
4.2	Supplier relationships in cloud services	2
4.3	Relationships between cloud service customers and cloud service providers.....	3
4.4	Managing information security risks in cloud services	3
4.5	Structure of this standard.....	3
5	Information security policies	4
5.1	Management direction for information security	4
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	6
7.3	Termination and 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 requirements of access control	8
9.2	User access management.....	9
9.3	User responsibilities	10
9.4	System and application access control	10
10	Cryptography.....	11
10.1	Cryptographic controls.....	11
11	Physical and environmental security	12
11.1	Secure areas.....	12
11.2	Equipment	12
12	Operations security.....	13
12.1	Operational procedures and responsibilities.....	13
12.2	Protection from malware.....	14
12.3	Backup	14
12.4	Logging and monitoring.....	15
12.5	Control of operational software.....	16
12.6	Technical vulnerability management	16
12.7	Information systems audit considerations	17

13	Communications security	17
	13.1 Network security management.....	17
	13.2 Information transfer.....	17
14	System acquisition, development and maintenance	18
	14.1 Security requirements of information systems	18
	14.2 Security in development and support processes	18
	14.3 Test data	19
15	Supplier relationships	19
	15.1 Information security in supplier relationships	19
	15.2 Supplier service delivery management.....	20
16	Information security incident management	20
	16.1 Management of information security incidents and improvements.....	20
17	Information security aspects of business continuity management.....	22
	17.1 Information security continuity	22
	17.2 Redundancies	22
18	Compliance.....	22
	18.1 Compliance with legal and contractual requirements.....	22
	18.2 Information security reviews.....	23
	Annex A – Cloud service extended control set.....	25
	Annex B – References on information security risk related to cloud computing	29
	Bibliography	30