

ISO/IEC 29151:2017-08 (E)

Information technology - Security techniques - Code of practice for personally identifiable information protection

Contents		Page
1	Scope	1
2	Normative references	1
3	Definitions and abbreviated terms	1
3.1	Definitions	1
3.2	Abbreviated terms	1
4	Overview	2
4.1	Objective for the protection of PII	2
4.2	Requirement for the protection of PII	2
4.3	Controls	2
4.4	Selecting controls	2
4.5	Developing organization specific guidelines	3
4.6	Life cycle considerations	3
4.7	Structure of this Specification	3
5	Information security policies	4
5.1	Management directions for information security	4
6	Organization of information security	4
6.1	Internal organization	4
6.2	Mobile devices and teleworking	5
7	Human resource security	6
7.1	Prior to employment	6
7.2	During employment	6
7.3	Termination and change of employment	6
8	Asset management	7
8.1	Responsibility for assets	7
8.2	Information classification	7
8.3	Media handling	8
9	Access control	9
9.1	Business requirement of access control	9
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	11
11.1	Secure areas	11
11.2	Equipment	12
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	14
12.6	Technical vulnerability management	14
12.7	Information systems audit considerations	14
13	Communications security	15
13.1	Network security management	15
13.2	Information transfer	15
14	System acquisition, development and maintenance	15
14.1	Security requirements of information systems	15
14.2	Security in development and support processes	16
iv Rec. ITU-T X.1058 (03/2017) 14.3 Test data		16
15	Supplier relationships	17
15.1	Information security in supplier relationships	17
15.2	Supplier service delivery management	18
16	Information security incident management	18
16.1	Management of information security incidents and improvements	18
17	Information security aspects of business continuity management	19
17.1	Information security continuity	19
17.2	Redundancies	19
18	Compliance	20
18.1	Compliance with legal and contractual requirements	20
18.2	Information security reviews	21
Annex A - Extended control set for PII protection (This annex forms an integral part of this Recommendation International Standard.)		22
A.1	General	22
A.2	General policies for the use and protection of PII	22
A.3	Consent and choice	22
A.4	Purpose legitimacy and specification	24
A.5	Collection limitation	26
A.6	Data minimization	26
A.7	Use, retention and disclosure limitation	27
A.8	Accuracy and quality	30
A.9	Openness, transparency and notice	31
A.10	PII principal participation and access	32
A.11	Accountability	34
A.12	Information security	37
A.13	Privacy compliance	37
Bibliography		39