

ISO/IEC 27018:2014-08 (E)

Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Contents		Page
Foreword		v
0	Introduction	vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Overview	3
4.1	Structure of this standard	3
4.2	Control categories	4
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	5
7	Human resource security	5
7.1	Prior to employment	5
7.2	During employment	5
7.3	Termination and change of employment	6
8	Asset management	6
9	Access control	6
9.1	Business requirements of access control	6
9.2	User access management	6
9.3	User responsibilities	7
9.4	System and application access control	7
10	Cryptography	8
10.1	Cryptographic controls	8
11	Physical and environmental security	8
11.1	Secure areas	8
11.2	Equipment	9
12	Operations security	9
12.1	Operational procedures and responsibilities	9
12.2	Protection from malware	10
12.3	Backup	10
12.4	Logging and monitoring	11
12.5	Control of operational software	12
12.6	Technical vulnerability management	12
12.7	Information systems audit considerations	12
13	Communications security	12

13.1	Network security management	12
13.2	Information transfer	12
14	System acquisition, development and maintenance	13
15	Supplier relationships	13
16	Information security incident management	13
16.1	Management of information security incidents and improvements	13
17	Information security aspects of business continuity management	14
18	Compliance	14
18.1	Compliance with legal and contractual requirements	14
18.2	Information security reviews	14
Annex A (normative) Public cloud PII processor extended control set for PII protection		15
Bibliography		23