

DIN ISO/IEC 27018:2017-08 (E)

Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (ISO/IEC 27018:2014)

Contents

| | Page |
|---|-----------|
| National foreword | 4 |
| National Annex (informative) Bibliography | 4 |
| Foreword | 5 |
| 0 Introduction | 6 |
| 1 Scope | 9 |
| 2 Normative references | 9 |
| 3 Terms and definitions | 9 |
| 4 Overview | 11 |
| 4.1 Structure of this standard | 11 |
| 4.2 Control categories | 12 |
| 5 Information security policies | 12 |
| 5.1 Management direction for information security | 12 |
| 6 Organization of information security | 13 |
| 6.1 Internal organization | 13 |
| 6.2 Mobile devices and teleworking | 13 |
| 7 Human resource security | 13 |
| 7.1 Prior to employment | 13 |
| 7.2 During employment | 13 |
| 7.3 Termination and change of employment | 14 |
| 8 Asset management | 14 |
| 9 Access control | 14 |
| 9.1 Business requirements of access control | 14 |
| 9.2 User access management | 14 |
| 9.3 User responsibilities | 15 |
| 9.4 System and application access control | 15 |
| 10 Cryptography | 16 |
| 10.1 Cryptographic controls | 16 |
| 11 Physical and environmental security | 16 |
| 11.1 Secure areas | 16 |
| 11.2 Equipment | 17 |
| 12 Operations security | 17 |
| 12.1 Operational procedures and responsibilities | 17 |
| 12.2 Protection from malware | 18 |
| 12.3 Backup | 18 |
| 12.4 Logging and monitoring | 19 |
| 12.5 Control of operational software | 20 |
| 12.6 Technical vulnerability management | 20 |
| 12.7 Information systems audit considerations | 20 |
| 13 Communications security | 20 |
| 13.1 Network security management | 20 |
| 13.2 Information transfer | 20 |

| | | |
|-----------|--|-----------|
| 14 | System acquisition, development and maintenance..... | 21 |
| 15 | Supplier relationships..... | 21 |
| 16 | Information security incident management..... | 21 |
| 16.1 | Management of information security incidents and improvements..... | 21 |
| 17 | Information security aspects of business continuity management..... | 22 |
| 18 | Compliance..... | 22 |
| 18.1 | Compliance with legal and contractual requirements..... | 22 |
| 18.2 | Information security reviews..... | 22 |
| | Annex A (normative) Public cloud PII processor extended control set for PII protection..... | 23 |
| | Bibliography..... | 31 |