

# ISO/IEC 27018:2019 (E)

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

---

### Contents

|       |  |
|-------|--|
|       | Foreword   |
|       | Introduction   |
| 1     | Scope  |
| 2     | Normative references                                     |
| 3     | Terms and definitions                                    |
| 4     | Overview   |
| 4.1   | Structure of this document                               |
| 4.2   | Control categories                                       |
| 5     | Information security policies                            |
| 5.1   | Management direction for information security            |
| 5.1.1 | Policies for information security                        |
| 5.1.2 | Review of the policies for information security          |
| 6     | Organization of information security                     |
| 6.1   | Internal organization                                    |
| 6.1.1 | Information security roles and responsibilities          |
| 6.1.2 | Segregation of duties                                    |
| 6.1.3 | Contact with authorities                                 |
| 6.1.4 | Contact with special interest groups                     |
| 6.1.5 | Information security in project management               |
| 6.2   | Mobile devices and teleworking                           |
| 7     | Human resource security                                  |
| 7.1   | Prior to employment                                      |
| 7.2   | During employment  |
| 7.2.1 | Management responsibilities                              |
| 7.2.2 | Information security awareness, education and training   |
| 7.2.3 | Disciplinary process                                     |
| 7.3   | Termination and change of employment                     |
| 8     | Asset management   |
| 9     | Access control   |
| 9.1   | Business requirements of access control                  |
| 9.2   | User access management                                   |
| 9.2.1 | User registration and de-registration                    |
| 9.2.2 | User access provisioning                                 |
| 9.2.3 | Management of privileged access rights                   |
| 9.2.4 | Management of secret authentication information of users |
| 9.2.5 | Review of user access rights                             |
| 9.2.6 | Removal or adjustment of access rights                   |
| 9.3   | User responsibilities                                    |
| 9.3.1 | Use of secret authentication information                 |
| 9.4   | System and application access control                    |
| 9.4.1 | Information access restriction                           |
| 9.4.2 | Secure log-on procedures                                 |

- 9.4.3 Password management system
- 9.4.4 Use of privileged utility programs
- 9.4.5 Access control to program source code
- 10 Cryptography
  - 10.1 Cryptographic controls
    - 10.1.1 Policy on the use of cryptographic controls
    - 10.1.2 Key management
- 11 Physical and environmental security
  - 11.1 Secure areas
  - 11.2 Equipment
    - 11.2.1 Equipment siting and protection
    - 11.2.2 Supporting utilities
    - 11.2.3 Cabling security
    - 11.2.4 Equipment maintenance
    - 11.2.5 Removal of assets
    - 11.2.6 Security of equipment and assets off-premises
    - 11.2.7 Secure disposal or re-use of equipment
    - 11.2.8 Unattended user equipment
    - 11.2.9 Clear desk and clear screen policy
- 12 Operations security
  - 12.1 Operational procedures and responsibilities
    - 12.1.1 Documented operating procedures
    - 12.1.2 Change management
    - 12.1.3 Capacity management
    - 12.1.4 Separation of development, testing and operational environments
  - 12.2 Protection from malware
  - 12.3 Backup
    - 12.3.1 Information backup
  - 12.4 Logging and monitoring
    - 12.4.1 Event logging
    - 12.4.2 Protection of log information
    - 12.4.3 Administrator and operator logs
    - 12.4.4 Clock synchronization
  - 12.5 Control of operational software
  - 12.6 Technical vulnerability management
  - 12.7 Information systems audit considerations
- 13 Communications security
  - 13.1 Network security management
  - 13.2 Information transfer
    - 13.2.1 Information transfer policies and procedures
    - 13.2.2 Agreements on information transfer
    - 13.2.3 Electronic messaging
    - 13.2.4 Confidentiality or non-disclosure agreements
- 14 System acquisition, development and maintenance
- 15 Supplier relationships
- 16 Information security incident management
  - 16.1 Management of information security incidents and improvements
    - 16.1.1 Responsibilities and procedures
    - 16.1.2 Reporting information security events
    - 16.1.3 Reporting information security weaknesses
    - 16.1.4 Assessment of and decision on information security events
    - 16.1.5 Response to information security incidents
    - 16.1.6 Learning from information security incidents
    - 16.1.7 Collection of evidence
- 17 Information security aspects of business continuity management

**18 Compliance**

- 18.1 Compliance with legal and contractual requirements**
- 18.2 Information security reviews**
  - 18.2.1 Independent review of information security**
  - 18.2.2 Compliance with security policies and standards**
  - 18.2.3 Technical compliance review**

**Annex A (normative) Public cloud PII processor extended control set for PII protection**

- A.1 General**
- A.2 Consent and choice**
  - A.2.1 Obligation to co-operate regarding PII principals' rights**
- A.3 Purpose legitimacy and specification**
  - A.3.1 Public cloud PII processor's purpose**
  - A.3.2 Public cloud PII processor's commercial use**
- A.4 Collection limitation**
- A.5 Data minimization**
  - A.5.1 Secure erasure of temporary files**
- A.6 Use, retention and disclosure limitation**
  - A.6.1 PII disclosure notification**
  - A.6.2 Recording of PII disclosures**
- A.7 Accuracy and quality**
- A.8 Openness, transparency and notice**
  - A.8.1 Disclosure of sub-contracted PII processing**
- A.9 Individual participation and access**
- A.10 Accountability**
  - A.10.1 Notification of a data breach involving PII**
  - A.10.2 Retention period for administrative security policies and guidelines**
  - A.10.3 PII return, transfer and disposal**
- A.11 Information security**
  - A.11.1 Confidentiality or non-disclosure agreements**
  - A.11.2 Restriction of the creation of hardcopy material**
  - A.11.3 Control and logging of data restoration**
  - A.11.4 Protecting data on storage media leaving the premises**
  - A.11.5 Use of unencrypted portable storage media and devices**
  - A.11.6 Encryption of PII transmitted over public data-transmission networks**
  - A.11.7 Secure disposal of hardcopy materials**
  - A.11.8 Unique use of user IDs**
  - A.11.9 Records of authorized users**
  - A.11.10 User ID management**
  - A.11.11 Contract measures**
  - A.11.12 Sub-contracted PII processing**
  - A.11.13 Access to data on pre-used data storage space**
- A.12 Privacy compliance**
  - A.12.1 Geographical location of PII**
  - A.12.2 Intended destination of PII**

Page count: 23