DIN EN ISO/IEC 27018:2020-08 (E)

Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (ISO/IEC 27018:20 19)

Contents

Page

European foreword ... **5**

Foreword ... **6**

Introduction ... **7**

1 Scope ... **10**

2 Normative references ... **10**

3 Terms and definitions ... **10**

4 Overview ... **12**
4.1 Structure of this document ... 12
4.2 Control categories ... 13

5 Information security policies ... **13**
5.1 Management direction for information security ... 13
5.1.1 Policies for information security ... 13
5.1.2 Review of the policies for information security ... 14

6 Organization of information security ... **14**
6.1 Internal organization ... 14
6.1.1 Information security roles and responsibilities ... 14
6.1.2 Segregation of duties ... 14
6.1.3 Contact with authorities ... 14
6.1.4 Contact with special interest groups ... 14
6.1.5 Information security in project management ... 14
6.2 Mobile devices and teleworking ... 14

7 Human resource security ... **14**
7.1 Prior to employment ... 14
7.2 During employment ... 14
7.2.1 Management responsibilities ... 15
7.2.2 Information security awareness, education and training ... 15
7.2.3 Disciplinary process ... 15
7.3 Termination and change of employment ... 15

8 Asset management ... **15**

9 Access control ... **15**
9.1 Business requirements of access control ... 15
9.2 User access management ... 15
9.2.1 User registration and de-registration ... 16
9.2.2 User access provisioning ... 16
9.2.3 Management of privileged access rights ... 16
9.2.4 Management of secret authentication information of users ... 16
9.2.5 Review of user access rights ... 16
9.2.6 Removal or adjustment of access rights ... 16
9.3 User responsibilities ... 16
9.3.1 Use of secret authentication information ... 16
9.4 System and application access control ... 16
9.4.1 Information access restriction ... 16
9.4.2 Secure log-on procedures ... 17
9.4.3 Password management system ... 17
9.4.4 Use of privileged utility programs ... 17
9.4.5 Access control to program source code ... 17

10 Cryptography **17**
10.1 Cryptographic controls 17
10.1.1 Policy on the use of cryptographic controls 17
10.1.2 Key management 17

11 Physical and environmental security **17**
11.1 Secure areas 17
11.2 Equipment 18
11.2.1 Equipment siting and protection 18
11.2.2 Supporting utilities 18
11.2.3 Cabling security 18
11.2.4 Equipment maintenance 18
11.2.5 Removal of assets 18
11.2.6 Security of equipment and assets off-premises 18
11.2.7 Secure disposal or re-use of equipment 18
11.2.8 Unattended user equipment 18
11.2.9 Clear desk and clear screen policy 18

12 Operations security **18**
12.1 Operational procedures and responsibilities 18
12.1.1 Documented operating procedures 19
12.1.2 Change management 19
12.1.3 Capacity management 19
12.1.4 Separation of development, testing and operational environments 19
12.2 Protection from malware 19
12.3 Backup 19
12.3.1 Information backup 19
12.4 Logging and monitoring 20
12.4.1 Event logging 20
12.4.2 Protection of log information 20
12.4.3 Administrator and operator logs 20
12.4.4 Clock synchronization 21
12.5 Control of operational software 21
12.6 Technical vulnerability management 21
12.7 Information systems audit considerations 21

13 Communications security **21**
13.1 Network security management 21
13.2 Information transfer 21
13.2.1 Information transfer policies and procedures 21
13.2.2 Agreements on information transfer 21
13.2.3 Electronic messaging 21
13.2.4 Confidentiality or non-disclosure agreements 21

14 System acquisition, development and maintenance **22**

15 Supplier relationships **22**

16 Information security incident management **22**
16.1 Management of information security incidents and improvements 22
16.1.1 Responsibilities and procedures 22
16.1.2 Reporting information security events 22
16.1.3 Reporting information security weaknesses 22
16.1.4 Assessment of and decision on information security events 22
16.1.5 Response to information security incidents 23
16.1.6 Learning from information security incidents 23
16.1.7 Collection of evidence 23

17 Information security aspects of business continuity management **23**

18 Compliance **23**
18.1 Compliance with legal and contractual requirements 23
18.2 Information security reviews 23
18.2.1 Independent review of information security 23
18.2.2 Compliance with security policies and standards 23
18.2.3 Technical compliance review 23

Annex A (normative) **Public cloud PII processor extended control set for PII protection** **24**

Bibliography **32**