DIN EN ISO/IEC 29151:2022-07 (E)

Information technology - Security techniques - Code of practice for personally identifiable information protection (ISO/IEC 29151:2017)

Contents

Page

European foreword 4

Foreword 5

Introduction 6

1 Scope 8

2 Normative references 8

3 Definitions and abbreviated terms 8

3.1 Definitions 8

3.2 Abbreviated terms 8

4 Overview 9

4.1 Objective for the protection of PII 9

4.2 Requirement for the protection of PII 9

4.3 Controls 9

4.4 Selecting controls 9

4.5 Developing organization specific guidelines 10

4.6 Life cycle considerations 10

4.7 Structure of this Specification 10

5 Information security policies 11

5.1 Management directions for information security 11

6 Organization of information security 11

6.1 Internal organization 11

6.2 Mobile devices and teleworking 12

7 Human resource security 13

7.1 Prior to employment 13

7.2 During employment 13

7.3 Termination and change of employment 13

8 Asset management 14

8.1 Responsibility for assets 14

8.2 Information classification 14

8.3 Media handling 15

9 Access control 16

9.1 Business requirement of access control 16

9.2 User access management 16

9.3 User responsibilities 17

9.4 System and application access control 17

10 Cryptography 18

10.1 Cryptographic controls 18

11 Physical and environmental security 18

11.1 Secure areas 18

11.2 Equipment 19

12 Operations security 19

12.1 Operational procedures and responsibilities 19

12.2 Protection from malware 20

12.3 Backup 20
12.4 Logging and monitoring 20
12.5 Control of operational software 21
12.6 Technical vulnerability management 21
12.7 Information systems audit considerations 21
13 Communications security 22
13.1 Network security management 22
13.2 Information transfer 22
14 System acquisition, development and maintenance 22
14.1 Security requirements of information systems 22
14.2 Security in development and support processes 23
14.3 Test data 23
15 Supplier relationships 24
15.1 Information security in supplier relationships 24
15.2 Supplier service delivery management 25
16 Information security incident management 25
16.1 Management of information security incidents and improvements 25
17 Information security aspects of business continuity management 26
17.1 Information security continuity 26
17.2 Redundancies 26
18 Compliance 27
18.1 Compliance with legal and contractual requirements 27
18.2 Information security reviews 28
Annex A – Extended control set for PII protection (This annex forms an integral part of this Recommendation | International Standard.) 29
A.1 General 29
A.2 General policies for the use and protection of PII 29
A.3 Consent and choice 29
A.4 Purpose legitimacy and specification 31
A.5 Collection limitation 33
A.6 Data minimization 33
A.7 Use, retention and disclosure limitation 34
A.8 Accuracy and quality 37
A.9 Openness, transparency and notice 38
A.10 PII principal participation and access 39
A.11 Accountability 41
A.12 Information security 44
A.13 Privacy compliance 44
Bibliography 46