ISO/IEC 27002:2013-10 (E)

Information technology - Security techniques - Code of practice for information security controls

Contents

Page

Foreword v

0 Introduction vi

1 Scope 1

2 Normative references 1

3 Termsanddefinitions 1

4 Structure of this standard 1
4.1 Clauses 1
4.2 Control categories 1

5 Information security policies 2
5.1 Management direction for information security 2

6 Organization of information security 4
6.1 Internal organization 4
6.2 Mobile devices and teleworking 6

7 Human resource security 9
7.1 Prior to employment 9
7.2 During employment 10
7.3 Termination and change of employment 13

8 Asset management 13
8.1 Responsibility for assets 13
8.2 Information classification 15
8.3 Media handling 17

9 Access control 19
9.1 Business requirements of access control 19
9.2 User access management 21
9.3 User responsibilities 24
9.4 System and application access control 25

10 Cryptography 28
10.1 Cryptographic controls 28

11 Physical and environmental security 30
11.1 Secure areas 30
11.2 Equipment 33

12 Operations security 38
12.1 Operational procedures and responsibilities 38
12.2 Protection from malware 41
12.3 Backup 42
12.4 Logging and monitoring 43
12.5 Control of operational software 45
12.6 Technical vulnerability management 46

12.7 Information systems audit considerations 48

13 Communications security 49
13.1 Network security management 49
13.2 Information transfer 50

14 System acquisition, development and maintenance 54
14.1 Security requirements of information systems 54
14.2 Security in development and support processes 57
14.3 Test data 62

15 Supplier relationships 62
15.1 Information security in supplier relationships 62
15.2 Supplier service delivery management 66

16 Information security incident management 67
16.1 Management of information security incidents and improvements 67

17 Information security aspects of business continuity management 71
17.1 Information security continuity 71
17.2 Redundancies 73

18 Compliance 74
18.1 Compliance with legal and contractual requirements 74
18.2 Information security reviews 77

Bibliography 79