DIN EN ISO/IEC 27017:2021-11 (E)

Information technology - Security techniques - Code of practice for information security controls based on ISO/I EC 27002 for cloud services (ISO/IEC 27017:2015)

Contents

Page

European foreword 4
Foreword 5
Introduction 6
1 Scope 7
2 Normative references 7
2.1 Identical Recommendations | International Standards 7
2.2 Additional References 7
3 Definitions and abbreviations 7
3.1 Terms defined elsewhere 7
3.2 Abbreviations 8
4 Cloud sector-specific concepts 8
4.1 Overview 8
4.2 Supplier relationships in cloud services 8
4.3 Relationships between cloud service customers and cloud service providers 9
4.4 Managing information security risks in cloud services 9
4.5 Structure of this standard 9
5 Information security policies 10
5.1 Management direction for information security 10
6 Organization of information security 11
6.1 Internal organization 11
6.2 Mobile devices and teleworking 12
7 Human resource security 12
7.1 Prior to employment 12
7.2 During employment 12
7.3 Termination and change of employment 13
8 Asset management 13
8.1 Responsibility for assets 13
8.2 Information classification 14
8.3 Media handling 14
9 Access control 14
9.1 Business requirements of access control 14
9.2 User access management 15
9.3 User responsibilities 16
9.4 System and application access control 16
10 Cryptography 17
10.1 Cryptographic controls 17
11 Physical and environmental security 18
11.1 Secure areas 18
11.2 Equipment 18
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 21

12.5 Control of operational software 22
12.6 Technical vulnerability management 22
12.7 Information systems audit considerations 23
13 Communications security 23
13.1 Network security management 23
13.2 Information transfer 23
14 System acquisition, development and maintenance 24
14.1 Security requirements of information systems 24
14.2 Security in development and support processes 24
14.3 Test data 25
15 Supplier relationships 25
15.1 Information security in supplier relationships 25
15.2 Supplier service delivery management 26
16 Information security incident management 26
16.1 Management of information security incidents and improvements 26
17 Information security aspects of business continuity management 28
17.1 Information security continuity 28
17.2 Redundancies 28
18 Compliance 28
18.1 Compliance with legal and contractual requirements 28
18.2 Information security reviews 29
Annex A – Cloud service extended control set 31
Annex B – References on information security risk related to cloud computing 35
Bibliography 36