ISO/IEC 27017:2026-07 (E)

Information security, cybersecurity and privacy protection - Information security controls based on ISO/IEC 27002 for cloud services

Contents

Page

Foreword vi

Introduction vii

1 Scope 1

2 Normative references 1

3 Terms,definitionsandabbreviatedterms 1
3.1 Terms and definitions 1
3.2 Abbreviated terms 2

4 Guidance for using this document 2
4.1 Relation between this document and ISO/IEC 27002:2022 2
4.2 Structure of this document 3
4.3 Cloud computing specific concepts 3
4.3.1 Supplier relationships in cloud services 3
4.3.2 Relationships between CSCs and CSPs 3
4.3.3 Managing information security risks in cloud services 4

5 Cloudservicespecificguidancerelatedtoorganizationalcontrols 5
5.1 Policies for information security 5
5.2 Information security roles and responsibilities 6
5.3 Segregation of duties 6
5.4 Management responsibilities 6
5.5 Contact with authorities 6
5.6 Contact with special interest groups 6
5.7 Threat intelligence 7
5.8 Information security in project management 7
5.9 Inventory of information and other associated assets 7
5.10 Acceptable use of information and other associated assets 7
5.11 Return of assets 8
5.12 Classification of information 8
5.13 Labelling of information 8
5.14 Information transfer 8
5.15 Access control 8
5.16 Identity management 8
5.17 Authentication information 9
5.18 Access rights 9
5.19 Information security in supplier relationships 9
5.20 Addressing information security within supplier agreements 10
5.21 Managing information security in the ICT supply chain 10
5.22 Monitoring, review and change management of supplier services 11
5.23 Information security for use of cloud services 11
5.24 Information security incident management planning and preparation 11
5.25 Assessment and decision on information security events 11
5.26 Response to information security incidents 12
5.27 Learning from information security incidents 12
5.28 Collection of evidence 12
5.29 Information security during disruption 12
5.30 ICT readiness for business continuity 12

5.31 Legal, statutory, regulatory and contractual requirements 13
5.32 Intellectual property rights 14
5.33 Protection of records 14
5.34 Privacy and protection of PII 14
5.35 Independent review of information security 14
5.36 Compliance with policies, rules and standards for information security 15
5.37 Documented operating procedures 15
5.38 CLD - Shared roles and responsibilities within a cloud computing environment 15
5.39 CLD - Agreement on the roles and responsibilities of the cloud service partner 16

6 Cloudservicespecificguidancerelatedtopeoplecontrols 17
6.1 Screening 17
6.2 Terms and conditions of employment 18
6.3 Information security awareness, education and training 18
6.4 Disciplinary process 18
6.5 Responsibilities after termination or change of employment 18
6.6 Confidentiality or non-disclosure agreements 18
6.7 Remote working 18
6.8 Information security event reporting 19

7 Cloudservicespecificguidancerelatedtophysicalcontrols 19
7.1 Physical security perimeters 19
7.2 Physical entry 19
7.3 Securing offices, rooms and facilities 19
7.4 Physical security monitoring 19
7.5 Protecting against physical and environmental threats 19
7.6 Working in secure areas 19
7.7 Clear desk and clear screen 19
7.8 Equipment siting and protection 19
7.9 Security of assets off-premises 20
7.10 Storage media 20
7.11 Supporting utilities 20
7.12 Cabling security 20
7.13 Equipment maintenance 20
7.14 Secure disposal or re-use of equipment 20

8 Cloudservicespecificguidancerelatedtotechnologicalcontrols 20
8.1 User endpoint devices 20
8.2 Privileged access rights 21
8.3 Information access restriction 21
8.4 Access to source code 21
8.5 Secure authentication 21
8.6 Capacity management 22
8.7 Protection against malware 22
8.8 Management of technical vulnerabilities 22
8.9 Configuration management 23
8.10 Information deletion 23
8.11 Data masking 24
8.12 Data leakage prevention 24
8.13 Information backup 24
8.14 Redundancy of information processing facilities 25
8.15 Logging 25
8.16 Monitoring activities 26
8.17 Clock synchronization 26
8.18 Use of privileged utility programs 27
8.19 Installation of software on operational systems 27
8.20 Network security 27
8.21 Security of network services 27
8.22 Segregation of networks 28
8.23 Web filtering 28

8.24 Use of cryptography 28
8.25 Secure development life cycle 28
8.26 Application security requirements 29
8.27 Secure system architecture and engineering principles 29
8.28 Secure coding 29
8.29 Security testing in development and acceptance 29
8.30 Outsourced development 29
8.31 Separation of development, test and production environments 29
8.32 Change management 29
8.33 Test information 30
8.34 Protection of information systems during audit and testing 30
8.35 CLD - Segregation in virtual computing environments 30
8.36 CLD - Detection and prevention of unauthorized use of cloud services 31

Annex A (Informative)Correspondencebetweenthisdocumentandthefirstedition(ISO/IEC 27017:2015) 33

Annex B (informative) Monitoring of cloud services 38

Bibliography 39