ISO/IEC 27011:2024-03 (E)

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

Contents

		Page
1	Scope	1
2	Normative references	1
3	Definitions and abbreviations	1
	3.1 Definitions	1
	3.2 Abbreviations	2
4	Overview	2
	4.1 Structure of this Recommendation | International Standard	2
	4.2 Information security management systems in telecommunications organizations	3
5	Organizational controls	5
	5.1 Policies for information security	5
	5.2 Information security roles and responsibilities	5
	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	6
	5.8 Information security in project management	6
	5.9 Inventory of information and other associated assets	6
	5.10 Acceptable use of information and other associated assets	6
	5.11 Return of assets	6
	5.12 Classification of information	7
	5.13 Labelling of information	7
	5.14 Information transfer	7
	5.15 Access control	7
	5.16 Identity management	7
	5.17 Authentication information	7
	5.18 Access rights	7
	5.19 Information security in supplier relationships	7
	5.20 Addressing information security within supplier agreements	8
	5.21 Managing information security in the ICT supply chain	8
	5.22 Monitoring, review and change management of supplier services	8
	5.23 Information security for use of cloud services	8
	5.24 Information security incident management planning and preparation	8
	5.25 Assessment and decision on information security events	9
	5.26 Response to information security incidents	9
	5.27 Learning from information security incidents	9
	5.28 Collection of evidence	9
	5.29 Information security during disruption	9

5.30 ICT readiness for business continuity 10
5.31 Legal, statutory, regulatory and contractual requirements 10
5.32 Intellectual property rights 10
5.33 Protection of records 10
5.34 Privacy and protection of PII 10
5.35 Independent review of information security 10
5.36 Compliance with policies, rules and standards for information security 10
5.37 Documented operating procedures 10
5.38 TEL – Interconnected telecommunications services 10
5.39 TEL – Security management of telecommunications services delivery 11
5.40 TEL – Response to spam 12
5.41 TEL – Response to DoS/DDoS attacks 12
5.42 TEL – Non-disclosure of communications 13
5.43 TEL – Essential communications 14
5.44 TEL – Legality of emergency actions 15
5.45 TEL – Coordination for information security incident management 15
People controls 16
6.1 Screening 16
6.2 Terms and conditions of employment 16
6.3 Information security awareness, education and training 16
6.4 Disciplinary process 16
6.5 Responsibilities after termination or change of employment 16
6.6 Confidentiality or non-disclosure agreements 16
6.7 Remote working 17
6.8 Information security event reporting 17
Physical controls 17
7.1 Physical security perimeter 17
7.2 Physical entry 17
7.3 Securing offices, rooms and facilities 17
7.4 Physical security monitoring 17
7.5 Protecting against physical and environmental threats 17
7.6 Working in secure areas 17
7.7 Clear desk and clear screen 17
7.8 Equipment siting and protection 18
7.9 Security of assets off-premises 18
7.10 Storage media 18
7.11 Supporting utilities 18
7.12 Cabling security 18
7.13 Equipment maintenance 18
7.14 Secure disposal or re-use of equipment 18
7.15 TEL – Securing communication centres 18
7.16 TEL – Securing telecommunications equipment room 19
7.17 TEL – Securing physically isolated operation areas 20
7.18 TEL – Equipment sited in other carriers' premises 21
7.19 TEL – Equipment sited in user premises 21
Technological controls 22
8.1 User endpoint devices 22
8.2 Privileged access rights 22
8.3 Information access restriction 22
8.4 Access to source code 22
8.5 Secure authentication 22

8.6 Capacity management 22
8.7 Protection against malware 22
8.8 Management of technical vulnerabilities 22
8.9 Configuration management 22
8.10 Information deletion 22
8.11 Data masking 22
8.12 Data leakage prevention 22
8.13 Information backup 22
8.14 Redundancy of information processing facilities 22
8.15 Logging 23
8.16 Monitoring activities 23
8.17 Clock synchronization 23
8.18 Use of privileged utility programs 23
8.19 Installation of software on operational systems 23
8.20 Network security 23
8.21 Security of network services 23
8.22 Segregation of networks 24
8.23 Web filtering 24
8.24 Use of cryptography 24
8.25 Secure development lifecycle 24
8.26 Application security requirements 24
8.27 Secure system architecture and engineering principles 24
8.28 Secure coding 24
8.29 Security testing in development and acceptance 24
8.30 Outsourced development 24
8.31 Separation of development, test and production environments 24
8.32 Change management 24
8.33 Test information 25
8.34 Protection of information systems during audit testing 25
8.35 TEL – Telecommunications carrier identification and authentication by users 25
Annex A Additional guidance for network security 26
A.1 Security measures against network attacks 26
A.2 Network security measures for network congestion 27
Bibliography 28