

DIN EN ISO/IEC 27011:2021-10 (E)

Information technology - Security techniques - Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations (ISO/IEC 27011:2016)

| Contents | | Page |
|--|--|-------------|
| European forward..... | | 4 |
| Forword..... | | 5 |
| Introduction..... | | 6 |
| 1 Scope..... | | 7 |
| 2 Normative references..... | | 7 |
| 3 Definitions and abbreviations..... | | 7 |
| 3.1 Definitions..... | | 7 |
| 3.2 Abbreviations..... | | 8 |
| 4 Overview..... | | 8 |
| 4.1 Structure of this Recommendation International Standard..... | | 8 |
| 4.2 Information security management systems in telecommunications organizations..... | | 9 |
| 5 Information security policies..... | | 11 |
| 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..... | | 13 |
| 7.3 Termination or 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 requirement for access control..... | | 14 |
| 9.2 User access management..... | | 15 |
| 9.3 User responsibilities..... | | 15 |
| 9.4 System and application access control..... | | 15 |
| 10 Cryptography..... | | 15 |
| 11 Physical and environmental security..... | | 15 |
| 11.1 Secure areas..... | | 15 |
| 11.2 Equipment..... | | 16 |
| 12 Operations security..... | | 18 |
| 12.1 Operational procedures and responsibilities..... | | 18 |
| 12.2 Protection from malware..... | | 19 |
| 12.3 Backup..... | | 19 |
| 12.4 Logging and monitoring..... | | 19 |
| 12.5 Control of operational software..... | | 19 |
| 12.6 Technical vulnerability management..... | | 20 |
| 12.7 Information systems audit considerations..... | | 20 |
| 13 Communications security..... | | 20 |
| 13.1 Network security management..... | | 20 |
| 13.2 Information transfer..... | | 21 |

| | | |
|------|---|----|
| 14 | System acquisition, development and maintenance | 22 |
| 14.1 | Security requirements of information systems | 22 |
| 14.2 | Security in development and support processes | 22 |
| 14.3 | Test data | 22 |
| 15 | Supplier relationships | 22 |
| 15.1 | Information security in supplier relationships | 22 |
| 15.2 | Supplier service delivery management..... | 23 |
| 16 | Information security incident management | 23 |
| 16.1 | Management of information security incidents and improvements..... | 23 |
| 17 | Information security aspects of business continuity management..... | 25 |
| 17.1 | Information security continuity | 25 |
| 17.2 | Redundancies | 26 |
| 18 | Compliance..... | 26 |
| | Annex A – Telecommunications extended control set | 27 |
| | Annex B – Additional guidance for network security | 35 |
| | B.1 Security measures against network attacks | 35 |
| | B.2 Network security measures for network congestion..... | 36 |
| | Bibliography | 37 |