ISO/IEC 27019:2024-10 (E)

Information security, cybersecurity and privacy protection - Information security controls for the energy utility industry

Contents

Page

Foreword ..... **vi**

Introduction ..... **vii**

1 Scope **1**

2 Normative references **2**

3 Terms, definitions and abbreviated terms **2**
3.1 Terms and definitions 2
3.2 Abbreviated terms 4

4 Structure of this document **4**

5 Organizational controls **4**
5.1 Policies for information security 4
5.2 Information security roles and responsibilities 4
5.3 Segregation of duties 4
5.4 Management responsibilities 4
5.5 Contact with authorities 5
5.6 Contact with special interest groups 5
5.7 Threat intelligence 5
5.8 Information security in project management 5
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 6
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 8
5.18 Access rights 8
5.19 Information security in supplier relationships 8
5.20 Addressing information security within supplier agreements 8
5.21 Managing information security in the ICT supply chain 9
5.22 Monitoring, review and change management of supplier services 9
5.23 Information security for use of cloud services 9
5.24 Information security incident management planning and preparation 9
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 9
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 ENR – Identification of risks related to external business partners 10
5.39 ENR – Addressing security when dealing with customers 11

6 People controls **12**
6.1 Screening 12
6.2 Terms and conditions of employment 12
6.3 Information security awareness, education and training 12
6.4 Disciplinary process 12
6.5 Responsibilities after termination or change of employment 12
6.6 Confidentiality or non-disclosure agreements 12
6.7 Remote working 13
6.8 Information security event reporting 13

7 Physical controls **13**
7.1 Physical security perimeters 13
7.2 Physical entry 13
7.3 Securing offices, rooms and facilities 13
7.4 Physical security monitoring 13
7.5 Protecting against physical and environmental threats 14
7.6 Working in secure areas 14
7.7 Clear desk and clear screen 14
7.8 Equipment siting and protection 14
7.9 Security of assets off-premises 14
7.10 Storage media 15
7.11 Supporting utilities 15
7.12 Cabling security 15
7.13 Equipment maintenance 15
7.14 Secure disposal or re-use of equipment 15
7.15 ENR – Securing control centres 15
7.16 ENR – Securing equipment rooms 16
7.17 ENR – Securing peripheral sites 18
7.18 ENR – Interconnected control and communication systems 18

8 Technological controls **19**
8.1 User endpoint devices 19
8.2 Privileged access rights 20
8.3 Information access restriction 20
8.4 Access to source code 20
8.5 Secure authentication 20
8.6 Capacity management 20
8.7 Protection against malware 20
8.8 Management of technical vulnerabilities 21
8.9 Configuration management 21
8.10 Information deletion 21
8.11 Data masking 21
8.12 Data leakage prevention 21
8.13 Information backup 21
8.14 Redundancy of information processing facilities 21
8.15 Logging 21
8.16 Monitoring activities 22
8.17 Clock synchronization 22
8.18 Use of privileged utility programs 22
8.19 Installation of software on operational systems 22
8.20 Networks security 22
8.21 Security of network services 22
8.22 Segregation of networks 23
8.23 Web filtering 23
8.24 Use of cryptography 23
8.25 Secure development life cycle 23
8.26 Application security requirements 23
8.27 Secure system architecture and engineering principles 23
8.28 Secure coding 23
8.29 Security testing in development and acceptance 23
8.30 Outsourced development 23
8.31 Separation of development, test and production environments 23
8.32 Change management 24
8.33 Test information 24
8.34 Protection of information systems during audit testing 24

8.35 ENR – Treatment of legacy systems 24
8.36 ENR – Integrity and availability of safety functions 25
8.37 ENR – Securing process control data communication 25
8.38 ENR – Logical connection of external process control systems 26
8.39 ENR – Least functionality 27
8.40 ENR – Emergency communication 27

Annex A (informative) **Energy utility industry specific controls reference** **29**

Annex B (informative) **Correspondence between this document and the first edition (ISO/IEC 27019:2017)** **30**

Bibliography **38**