

DIN EN ISO/IEC 27019:2020-08 (E)

Information technology - Security techniques - Information security controls for the energy utility industry (ISO/IEC 27019:201 7, Corrected version 2019-08)

Contents

Page

European foreword	6
Foreword	7
0 Introduction	8
1 Scope	11
2 Normative references	11
3 Terms and definitions	12
4 Structure of the document	14
4.1 General	14
4.2 Refinement of ISO/IEC 27001:2013 requirements	14
4.3 Energy utility industry specific guidance related to ISO/IEC 27002:2013	14
5 Information security policies	14
6 Organization of information security	14
6.1 Internal organization	14
6.1.1 Information security roles and responsibilities	14
6.1.2 Segregation of duties	15
6.1.3 Contact with authorities	15
6.1.4 Contact with special interest groups	15
6.1.5 Information security in project management	15
6.1.6 ENR – Identification of risks related to external parties	15
6.1.7 ENR – Addressing security when dealing with customers	16
6.2 Mobile devices and teleworking	16
6.2.1 Mobile device policy	16
6.2.2 Teleworking	17
7 Human resource security	17
7.1 Prior to employment	17
7.1.1 Screening	17
7.1.2 Terms and conditions of employment	18
7.2 During employment	18
7.2.1 Management responsibilities	18
7.2.2 Information security awareness, education and training	18
7.2.3 Disciplinary process	18
7.3 Termination and change of employment	18
8 Asset management	18
8.1 Responsibility for assets	18
8.1.1 Inventory of assets	18
8.1.2 Ownership of assets	19
8.1.3 Acceptable use of assets	19
8.1.4 Return of assets	19
8.2 Information classification	19
8.2.1 Classification of information	19
8.2.2 Labelling of information	20
8.2.3 Handling of assets	20
8.3 Media handling	20
9 Access control	20
9.1 Business requirements of access control	20
9.1.1 Access control policy	20
9.1.2 Access to networks and network services	20
9.2 User access management	21
9.2.1 User registration and de-registration	21
9.2.2 User access provisioning	21
9.2.3 Management of privileged access rights	21

9.2.4	Management of secret authentication information of users.....	21
9.2.5	Review of user access rights.....	21
9.2.6	Removal or adjustment of access rights.....	21
9.3	User responsibilities.....	21
9.3.1	Use of secret authentication information.....	21
9.4	System and application access control.....	22
9.4.1	Information access restriction.....	22
9.4.2	Secure log-on procedures.....	22
9.4.3	Password management system.....	22
9.4.4	Use of privileged utility programs.....	22
9.4.5	Access control to program source code.....	22
10	Cryptography.....	22
10.1	Cryptography controls.....	22
10.1.1	Policy on the use of cryptographic controls.....	22
10.1.2	Key management.....	22
11	Physical and environmental security.....	23
11.1	Secure areas.....	23
11.1.1	Physical security perimeter.....	23
11.1.2	Physical entry controls.....	23
11.1.3	Securing offices, rooms and facilities.....	23
11.1.4	Protecting against external and environmental threats.....	23
11.1.5	Working in secure areas.....	23
11.1.6	Delivery and loading areas.....	23
11.1.7	ENR – Securing control centres.....	23
11.1.8	ENR – Securing equipment rooms.....	24
11.1.9	ENR – Securing peripheral sites.....	25
11.2	Equipment.....	26
11.2.1	Equipment siting and protection.....	26
11.2.2	Supporting utilities.....	26
11.2.3	Cabling security.....	26
11.2.4	Equipment maintenance.....	26
11.2.5	Removal of assets.....	26
11.2.6	Security of equipment and assets off-premises.....	27
11.2.7	Secure disposal or re-use of equipment.....	27
11.2.8	Unattended user equipment.....	27
11.2.9	Clear desk and clear screen policy.....	27
11.3	ENR – Security in premises of external parties.....	27
11.3.1	ENR – Equipment sited on the premises of other energy utility organizations.....	27
11.3.2	ENR – Equipment sited on customer’s premises.....	28
11.3.3	ENR – Interconnected control and communication systems.....	28
12	Operations security.....	28
12.1	Operational procedures and responsibilities.....	28
12.1.1	Documented operating procedures.....	28
12.1.2	Change management.....	29
12.1.3	Capacity management.....	29
12.1.4	Separation of development, testing and operational environments.....	29
12.2	Protection from malware.....	29
12.2.1	Controls against malware.....	29
12.3	Back-up.....	30
12.4	Logging and monitoring.....	30
12.4.1	Event logging.....	30
12.4.2	Protection of log information.....	30
12.4.3	Administrator and operator logs.....	30
12.4.4	Clock synchronization.....	30
12.5	Control of operational software.....	30
12.5.1	Installation of software on operational systems.....	30
12.6	Technical vulnerability management.....	31

12.6.1	Management of technical vulnerabilities.....	31
12.6.2	Restrictions on software installation.....	31
12.7	Information systems audit considerations.....	31
12.8	ENR – Legacy systems.....	31
12.8.1	ENR – Treatment of legacy systems.....	31
12.9	ENR – Safety functions.....	32
12.9.1	ENR – Integrity and availability of safety functions.....	32
13	Communications security.....	32
13.1	Network security management.....	32
13.1.1	Network controls.....	32
13.1.2	Security of network services.....	32
13.1.3	Segregation in networks.....	32
13.1.4	ENR – Securing process control data communication.....	33
13.1.5	ENR – Logical connection of external process control systems.....	33
13.2	Information transfer.....	34
14	System acquisition, development and maintenance.....	34
14.1	Security requirements of information systems.....	34
14.1.1	Information security requirements analysis and specification.....	34
14.1.2	Securing application services on public networks.....	34
14.1.3	Protecting application services transactions.....	34
14.2	Security in development and support processes.....	34
14.2.1	Secure development policy.....	34
14.2.2	System change control procedures.....	34
14.2.3	Technical review of applications after operating platform changes.....	34
14.2.4	Restrictions on changes to software packages.....	34
14.2.5	Secure system engineering principles.....	34
14.2.6	Secure development environment.....	34
14.2.7	Outsourced development.....	34
14.2.8	System security testing.....	35
14.2.9	System acceptance testing.....	35
14.2.10	ENR – Least functionality.....	35
14.3	Test data.....	35
15	Supplier relationships.....	35
15.1	Information security in supplier relationships.....	35
15.1.1	Information security policy for supplier relationships.....	35
15.1.2	Addressing security within supplier agreements.....	35
15.1.3	Information and communication technology supply chain.....	35
15.2	Supplier service delivery management.....	36
16	Information security incident management.....	36
16.1	Management of information security incidents and improvements.....	36
16.1.1	Responsibilities and procedures.....	36
16.1.2	Reporting information security events.....	36
16.1.3	Reporting information security weaknesses.....	36
16.1.4	Assessment of and decision on information security events.....	36
16.1.5	Response to information security incidents.....	36
16.1.6	Learning from information security incidents.....	36
16.1.7	Collection of evidence.....	36
17	Information security aspects of business continuity management.....	36
17.1	Information security continuity.....	36
17.2	Redundancies.....	36
17.2.1	Availability of information processing facilities.....	36
17.2.2	ENR – Emergency communication.....	37
18	Compliance.....	38
18.1	Compliance with legal and contractual requirements.....	38
18.1.1	Identification of applicable legislation and contractual requirements.....	38

18.1.2	Intellectual property rights	38
18.1.3	Protection of records.....	38
18.1.4	Privacy and protection of personally identifiable information	38
18.1.5	Regulation of cryptographic controls	38
18.2	Information security reviews.....	38
18.2.1	Independent review of information security.....	38
18.2.2	Compliance with security policies and standards	38
18.2.3	Technical compliance review	39
Annex A (normative) Energy utility industry specific reference control objectives and controls....		40
Bibliography		43