

SLOVENSKI STANDARD

SIST EN ISO/IEC 27019:2020

01-maj-2020

Informacijska tehnologija - Varnostne tehnike - Kontrole informacijske varnosti za energetske operaterje (ISO/IEC 27019:2017, popravljena različica 2019-08)

Information technology - Security techniques - Information security controls for the energy utility industry (ISO/IEC 27019:2017, Corrected version 2019-08)

Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmaßnahmen für die Energieversorgung (ISO/IEC 27019:2017, korrigierte Fassung 2019-08)

Technologies de l'information - Techniques de sécurité - Mesures de sécurité de l'information pour l'industrie des opérateurs de l'énergie (ISO/IEC 27019:2017, Version corrigée 2019-08)

<https://standards.iteh.ai/catalog/standards/sist/619d09cb-7da7-405a-9b50-2d94beb3d61f/sist-en-iso-iec-27019-2020>

Ta slovenski standard je istoveten z: EN ISO/IEC 27019:2020

ICS:

03.100.70	Sistemi vodenja	Management systems
27.010	Prenos energije in toplote na splošno	Energy and heat transfer engineering in general
35.030	Informacijska varnost	IT Security

SIST EN ISO/IEC 27019:2020

en,fr,de

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN ISO/IEC 27019:2020

<https://standards.iteh.ai/catalog/standards/sist/619d09cb-7da7-405a-9b50-2d94beb3d61f/sist-en-iso-iec-27019-2020>

EUROPEAN STANDARD

EN ISO/IEC 27019

NORME EUROPÉENNE

EUROPÄISCHE NORM

March 2020

ICS 03.100.70

English version

Information technology - Security techniques - Information security controls for the energy utility industry (ISO/IEC 27019:2017, Corrected version 2019-08)

Technologies de l'information - Techniques de sécurité
- Mesures de sécurité de l'information pour l'industrie
des opérateurs de l'énergie (ISO/IEC 27019:2017,
Version corrigée 2019-08)

Informationstechnik - Sicherheitsverfahren -
Informationssicherheitsmaßnahmen für die
Energieversorgung (ISO/IEC 27019:2017, korrigierte
Fassung 2019-08)

This European Standard was approved by CEN on 2 March 2020.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Contents	Page
European foreword.....	3

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN ISO/IEC 27019:2020
<https://standards.iteh.ai/catalog/standards/sist/619d09cb-7da7-405a-9b50-2d94beb3d61f/sist-en-iso-iec-27019-2020>

European foreword

The text of ISO/IEC 27019:2017 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 27019:2020 by Technical Committee CEN/CLC/JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by September 2020, and conflicting national standards shall be withdrawn at the latest by September 2020.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

iTeh STANDARD PREVIEW Endorsement notice (standards.iteh.ai)

The text of ISO/IEC 27019:2017 has been approved by CEN as EN ISO/IEC 27019:2020 without any modification.

SIST EN ISO/IEC 27019:2020

<https://standards.iteh.ai/catalog/standards/sist/619d09cb-7da7-405a-9b50-2d94beb3d61f/sist-en-iso-iec-27019-2020>

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN ISO/IEC 27019:2020

<https://standards.iteh.ai/catalog/standards/sist/619d09cb-7da7-405a-9b50-2d94beb3d61f/sist-en-iso-iec-27019-2020>

INTERNATIONAL STANDARD

**ISO/IEC
27019**

First edition
2017-10

Corrected version
2019-08

Information technology — Security techniques — Information security controls for the energy utility industry

*Technologies de l'information — Techniques de sécurité — Mesures
de sécurité de l'information pour l'industrie des opérateurs de
l'énergie*

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST EN ISO/IEC 27019:2020](https://standards.iteh.ai/catalog/standards/sist/619d09cb-7da7-405a-9b50-2d94beb3d61f/sist-en-iso-iec-27019-2020)

[https://standards.iteh.ai/catalog/standards/sist/619d09cb-7da7-405a-9b50-
2d94beb3d61f/sist-en-iso-iec-27019-2020](https://standards.iteh.ai/catalog/standards/sist/619d09cb-7da7-405a-9b50-2d94beb3d61f/sist-en-iso-iec-27019-2020)



Reference number
ISO/IEC 27019:2017(E)

© ISO/IEC 2017

iTeh STANDARD PREVIEW (standards.iteh.ai)

SIST EN ISO/IEC 27019:2020

<https://standards.iteh.ai/catalog/standards/sist/619d09cb-7da7-405a-9b50-2d94beb3d61f/sist-en-iso-iec-27019-2020>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

	Page
Foreword	vii
0	viii
Introduction	viii
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Structure of the document	4
4.1 General	4
4.2 Refinement of ISO/IEC 27001:2013 requirements	4
4.3 Energy utility industry specific guidance related to ISO/IEC 27002:2013	4
5 Information security policies	4
6 Organization of information security	4
6.1 Internal organization	4
6.1.1 Information security roles and responsibilities	4
6.1.2 Segregation of duties	5
6.1.3 Contact with authorities	5
6.1.4 Contact with special interest groups	5
6.1.5 Information security in project management	5
6.1.6 ENR – Identification of risks related to external parties	5
6.1.7 ENR – Addressing security when dealing with customers	6
6.2 Mobile devices and teleworking	6
6.2.1 Mobile device policy	6
6.2.2 Teleworking	7
7 Human resource security	7
7.1 Prior to employment	7
7.1.1 Screening	7
7.1.2 Terms and conditions of employment	8
7.2 During employment	8
7.2.1 Management responsibilities	8
7.2.2 Information security awareness, education and training	8
7.2.3 Disciplinary process	8
7.3 Termination and change of employment	8
8 Asset management	8
8.1 Responsibility for assets	8
8.1.1 Inventory of assets	8
8.1.2 Ownership of assets	9
8.1.3 Acceptable use of assets	9
8.1.4 Return of assets	9
8.2 Information classification	9
8.2.1 Classification of information	9
8.2.2 Labelling of information	10
8.2.3 Handling of assets	10
8.3 Media handling	10
9 Access control	10
9.1 Business requirements of access control	10
9.1.1 Access control policy	10
9.1.2 Access to networks and network services	10
9.2 User access management	11
9.2.1 User registration and de-registration	11
9.2.2 User access provisioning	11
9.2.3 Management of privileged access rights	11

ISO/IEC 27019:2017(E)

9.2.4	Management of secret authentication information of users.....	11
9.2.5	Review of user access rights.....	11
9.2.6	Removal or adjustment of access rights.....	11
9.3	User responsibilities.....	11
9.3.1	Use of secret authentication information.....	11
9.4	System and application access control.....	12
9.4.1	Information access restriction.....	12
9.4.2	Secure log-on procedures.....	12
9.4.3	Password management system.....	12
9.4.4	Use of privileged utility programs.....	12
9.4.5	Access control to program source code.....	12
10	Cryptography.....	12
10.1	Cryptography controls.....	12
10.1.1	Policy on the use of cryptographic controls.....	12
10.1.2	Key management.....	12
11	Physical and environmental security.....	13
11.1	Secure areas.....	13
11.1.1	Physical security perimeter.....	13
11.1.2	Physical entry controls.....	13
11.1.3	Securing offices, rooms and facilities.....	13
11.1.4	Protecting against external and environmental threats.....	13
11.1.5	Working in secure areas.....	13
11.1.6	Delivery and loading areas.....	13
11.1.7	ENR – Securing control centres.....	13
11.1.8	ENR – Securing equipment rooms.....	14
11.1.9	ENR – Securing peripheral sites.....	15
11.2	Equipment.....	16
11.2.1	Equipment siting and protection.....	16
11.2.2	Supporting utilities.....	16
11.2.3	Cabling security.....	16
11.2.4	Equipment maintenance.....	16
11.2.5	Removal of assets.....	16
11.2.6	Security of equipment and assets off-premises.....	17
11.2.7	Secure disposal or re-use of equipment.....	17
11.2.8	Unattended user equipment.....	17
11.2.9	Clear desk and clear screen policy.....	17
11.3	ENR – Security in premises of external parties.....	17
11.3.1	ENR – Equipment sited on the premises of other energy utility organizations.....	17
11.3.2	ENR – Equipment sited on customer’s premises.....	18
11.3.3	ENR – Interconnected control and communication systems.....	18
12	Operations security.....	18
12.1	Operational procedures and responsibilities.....	18
12.1.1	Documented operating procedures.....	18
12.1.2	Change management.....	19
12.1.3	Capacity management.....	19
12.1.4	Separation of development, testing and operational environments.....	19
12.2	Protection from malware.....	19
12.2.1	Controls against malware.....	19
12.3	Back-up.....	20
12.4	Logging and monitoring.....	20
12.4.1	Event logging.....	20
12.4.2	Protection of log information.....	20
12.4.3	Administrator and operator logs.....	20
12.4.4	Clock synchronization.....	20
12.5	Control of operational software.....	20
12.5.1	Installation of software on operational systems.....	20
12.6	Technical vulnerability management.....	21

12.6.1	Management of technical vulnerabilities.....	21
12.6.2	Restrictions on software installation.....	21
12.7	Information systems audit considerations.....	21
12.8	ENR – Legacy systems.....	21
12.8.1	ENR – Treatment of legacy systems.....	21
12.9	ENR – Safety functions.....	22
12.9.1	ENR – Integrity and availability of safety functions.....	22
13	Communications security.....	22
13.1	Network security management.....	22
13.1.1	Network controls.....	22
13.1.2	Security of network services.....	22
13.1.3	Segregation in networks.....	22
13.1.4	ENR – Securing process control data communication.....	23
13.1.5	ENR – Logical connection of external process control systems.....	23
13.2	Information transfer.....	24
14	System acquisition, development and maintenance.....	24
14.1	Security requirements of information systems.....	24
14.1.1	Information security requirements analysis and specification.....	24
14.1.2	Securing application services on public networks.....	24
14.1.3	Protecting application services transactions.....	24
14.2	Security in development and support processes.....	24
14.2.1	Secure development policy.....	24
14.2.2	System change control procedures.....	24
14.2.3	Technical review of applications after operating platform changes.....	24
14.2.4	Restrictions on changes to software packages.....	24
14.2.5	Secure system engineering principles.....	24
14.2.6	Secure development environment.....	24
14.2.7	Outsourced development.....	24
14.2.8	System security testing.....	25
14.2.9	System acceptance testing.....	25
14.2.10	ENR – Least functionality.....	25
14.3	Test data.....	25
15	Supplier relationships.....	25
15.1	Information security in supplier relationships.....	25
15.1.1	Information security policy for supplier relationships.....	25
15.1.2	Addressing security within supplier agreements.....	25
15.1.3	Information and communication technology supply chain.....	25
15.2	Supplier service delivery management.....	26
16	Information security incident management.....	26
16.1	Management of information security incidents and improvements.....	26
16.1.1	Responsibilities and procedures.....	26
16.1.2	Reporting information security events.....	26
16.1.3	Reporting information security weaknesses.....	26
16.1.4	Assessment of and decision on information security events.....	26
16.1.5	Response to information security incidents.....	26
16.1.6	Learning from information security incidents.....	26
16.1.7	Collection of evidence.....	26
17	Information security aspects of business continuity management.....	26
17.1	Information security continuity.....	26
17.2	Redundancies.....	26
17.2.1	Availability of information processing facilities.....	26
17.2.2	ENR – Emergency communication.....	27
18	Compliance.....	28
18.1	Compliance with legal and contractual requirements.....	28
18.1.1	Identification of applicable legislation and contractual requirements.....	28

ISO/IEC 27019:2017(E)

18.1.2	Intellectual property rights	28
18.1.3	Protection of records	28
18.1.4	Privacy and protection of personally identifiable information	28
18.1.5	Regulation of cryptographic controls	28
18.2	Information security reviews	28
18.2.1	Independent review of information security	28
18.2.2	Compliance with security policies and standards	28
18.2.3	Technical compliance review	29
Annex A (normative) Energy utility industry specific reference control objectives and controls		30
Bibliography		33

iTeh STANDARD PREVIEW (standards.iteh.ai)

SIST EN ISO/IEC 27019:2020

<https://standards.iteh.ai/catalog/standards/sist/619d09cb-7da7-405a-9b50-2d94beb3d61f/sist-en-iso-iec-27019-2020>

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This first edition cancels and replaces the first edition of ISO/IEC TR 27019:2013, which has been technically revised.

The main changes compared to the previous edition are as follows:

- the scope has changed to include the energy oil sector;
- this document has been changed from a Technical Report to an International Standard;
- the previous edition was aligned with ISO/IEC 27002:2005. The new structure has been aligned with ISO/IEC 27002:2013;
- the title has been changed.
- where appropriate the technical content has been revised and updated to reflect current technological developments in the energy sector.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

This corrected version of ISO 27019:2017 corrects "should" into "shall" in [Table A.1](#), 11.1.7