

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 Standards
(<https://standards.iteh.ai>)
Document Preview

[ISO/IEC 27019:2017](https://standards.iteh.ai/catalog/standards/iso/7b2ffddf-c361-467c-a8c5-4c9f200f9cfa/iso-iec-27019-2017)

<https://standards.iteh.ai/catalog/standards/iso/7b2ffddf-c361-467c-a8c5-4c9f200f9cfa/iso-iec-27019-2017>



Reference number
ISO/IEC 27019:2017(E)

© ISO/IEC 2017

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

ISO/IEC 27019:2017

<https://standards.itih.ai/catalog/standards/iso/7b2ffddf-c361-467c-a8c5-4c9f200f9cfa/iso-iec-27019-2017>



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

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

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 Standards
(<https://standards.iteh.ai>)
Document Preview

[ISO/IEC 27019:2017](https://standards.iteh.ai/catalog/standards/iso/7b2ffdff-c361-467c-a8c5-4c9f200f9cfa/iso-iec-27019-2017)

<https://standards.iteh.ai/catalog/standards/iso/7b2ffdff-c361-467c-a8c5-4c9f200f9cfa/iso-iec-27019-2017>