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

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

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>



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>



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2017

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
Fax: +41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos	vii
0 Introduction	viii
1 Domaine d'application	1
2 Références normatives	2
3 Termes et définitions	2
4 Structure du document	4
4.1 Généralités	4
4.2 Affinage des exigences de l'ISO/IEC 27001:2013	4
4.3 Recommandations spécifiques à l'industrie des opérateurs de l'énergie relatives à l'ISO/IEC 27002:2013	5
5 Politiques de sécurité de l'information	5
6 Organisation de la sécurité de l'information	5
6.1 Organisation interne	5
6.1.1 Fonctions et responsabilités liées à la sécurité de l'information	5
6.1.2 Séparation des tâches	5
6.1.3 Relations avec les autorités	5
6.1.4 Relations avec des groupes de travail spécialisés	6
6.1.5 La sécurité de l'information dans la gestion de projet	6
6.1.6 ENR – Identification des risques relatifs aux tiers	6
6.1.7 ENR – La sécurité avec les clients	7
6.2 Appareils mobiles et télétravail	7
6.2.1 Politique en matière d'appareils mobiles	7
6.2.2 Télétravail	8
7 La sécurité des ressources humaines	8
7.1 Avant l'embauche	8
7.1.1 Sélection des candidats	8
7.1.2 Termes et conditions d'embauche	8
7.2 Pendant la durée du contrat	9
7.2.1 Responsabilités de la direction	9
7.2.2 Sensibilisation, apprentissage et formation à la sécurité de l'information	9
7.2.3 Processus disciplinaire	9
7.3 Rupture, terme ou modification du contrat de travail	9
8 Gestion des actifs	9
8.1 Responsabilités relatives aux actifs	9
8.1.1 Inventaire des actifs	9
8.1.2 Propriété des actifs	10
8.1.3 Utilisation correcte des actifs	10
8.1.4 Restitution des actifs	10
8.2 Classification de l'information	10
8.2.1 Classification des informations	10
8.2.2 Marquage des informations	11
8.2.3 Manipulation des actifs	11
8.3 Manipulation des supports	11
9 Contrôle d'accès	11
9.1 Exigences métier en matière de contrôle d'accès	11
9.1.1 Politique de contrôle d'accès	11
9.1.2 Accès aux réseaux et aux services en réseau	11
9.2 Gestion de l'accès utilisateur	12
9.2.1 Enregistrement et désinscription des utilisateurs	12
9.2.2 Maîtrise de la gestion des accès utilisateur	12
9.2.3 Gestion des privilèges d'accès	12

9.2.4	Gestion des informations secrètes d'authentification des utilisateurs.....	12
9.2.5	Revue des droits d'accès utilisateur.....	12
9.2.6	Suppression ou adaptation des droits d'accès.....	12
9.3	Responsabilités des utilisateurs.....	12
9.3.1	Utilisation d'informations secrètes d'authentification	12
9.4	Contrôle de l'accès au système et aux applications.....	13
9.4.1	Restriction d'accès à l'information.....	13
9.4.2	Sécuriser les procédures de connexion.....	13
9.4.3	Système de gestion des mots de passe.....	13
9.4.4	Utilisation de programmes utilitaires à privilèges.....	13
9.4.5	Contrôle d'accès au code source des programmes.....	14
10	Cryptographie.....	14
10.1	Mesures cryptographiques.....	14
10.1.1	Politique d'utilisation des mesures cryptographiques.....	14
10.1.2	Gestion des clés.....	14
11	Sécurité physique et environnementale	14
11.1	Zones sécurisées.....	14
11.1.1	Périmètre de sécurité physique.....	14
11.1.2	Contrôles physiques des accès.....	14
11.1.3	Sécurisation des bureaux, des salles et des équipements.....	14
11.1.4	Protection contre les menaces extérieures et environnementales	15
11.1.5	Travail dans les zones sécurisées.....	15
11.1.6	Zones de livraison et de chargement.....	15
11.1.7	ENR – Sécurisation des centres de contrôle.....	15
11.1.8	ENR – Sécurisation des salles d'équipements.....	16
11.1.9	ENR – Sécurisation des sites périphériques.....	17
11.2	Matériels.....	18
11.2.1	Emplacement et protection du matériel.....	18
11.2.2	Services généraux.....	18
11.2.3	Sécurité du câblage.....	18
11.2.4	Maintenance du matériel.....	18
11.2.5	Sortie des actifs.....	18
11.2.6	Sécurité du matériel et des actifs hors des locaux.....	19
11.2.7	Mise au rebut ou recyclage sécurisé(e) du matériel	19
11.2.8	Matériel utilisateur laissé sans surveillance.....	19
11.2.9	Politique du bureau propre et de l'écran vide.....	19
11.3	ENR – Sécurité dans les locaux de tiers.....	19
11.3.1	ENR – Équipements situés dans les locaux d'autres opérateurs de l'énergie.....	19
11.3.2	ENR – Équipements situés dans les locaux du client.....	20
11.3.3	ENR – Systèmes de contrôle et de communication interconnectés.....	20
12	Sécurité liée à l'exploitation.....	21
12.1	Procédures et responsabilités liées à l'exploitation.....	21
12.1.1	Procédures d'exploitation documentées.....	21
12.1.2	Gestion des changements.....	21
12.1.3	Dimensionnement.....	21
12.1.4	Séparation des environnements de développement, de test et d'exploitation	21
12.2	Protection contre les logiciels malveillants.....	21
12.2.1	Mesures contre les logiciels malveillants	21
12.3	Sauvegarde.....	22
12.4	Journalisation et surveillance.....	22
12.4.1	Journalisation des événements.....	22
12.4.2	Protection de l'information journalisée.....	22
12.4.3	Journaux administrateur et opérateur.....	22
12.4.4	Synchronisation des horloges	22
12.5	Maîtrise des logiciels en exploitation.....	23
12.5.1	Installation de logiciels sur des systèmes en exploitation.....	23
12.6	Gestion des vulnérabilités techniques.....	23

12.6.1	Gestion des vulnérabilités techniques.....	23
12.6.2	Restrictions liées à l'installation de logiciels.....	23
12.7	Considérations sur l'audit du système d'information.....	23
12.8	ENR – Systèmes existants.....	24
12.8.1	ENR – Traitement des systèmes existants.....	24
12.9	ENR – Fonctions de sûreté.....	24
12.9.1	ENR – Intégrité et disponibilité des fonctions de sûreté.....	24
13	Sécurité des communications.....	25
13.1	Management de la sécurité des réseaux.....	25
13.1.1	Contrôle des réseaux.....	25
13.1.2	Sécurité des services de réseau.....	25
13.1.3	Cloisonnement des réseaux.....	25
13.1.4	ENR – Sécurisation des communications de données de contrôle des processus.....	25
13.1.5	ENR – Connexion logique des systèmes de contrôle des processus externes.....	26
13.2	Transfert de l'information.....	26
14	Acquisition, développement et maintenance des systèmes d'information.....	27
14.1	Exigences de sécurité applicables aux systèmes d'information.....	27
14.1.1	Analyse et spécification des exigences de sécurité de l'information.....	27
14.1.2	Sécurisation des services d'application sur les réseaux publics.....	27
14.1.3	Protection des transactions liées aux services d'application.....	27
14.2	Sécurité des processus de développement et d'assistance technique.....	27
14.2.1	Politique de développement sécurisé.....	27
14.2.2	Procédures de contrôle des changements apportés au système.....	27
14.2.3	Revue technique des applications après changement apporté à la plateforme d'exploitation.....	27
14.2.4	Restrictions relatives aux changements apportés aux progiciels.....	27
14.2.5	Principes d'ingénierie de la sécurité des systèmes.....	27
14.2.6	Environnement de développement sécurisé.....	27
14.2.7	Développement externalisé.....	28
14.2.8	Phase de test de la sécurité du système.....	28
14.2.9	Test de conformité du système.....	28
14.2.10	ENR – Moindre fonctionnalité.....	28
14.3	Données de test.....	28
15	Relations avec les fournisseurs.....	28
15.1	Sécurité de l'information dans les relations avec les fournisseurs.....	28
15.1.1	Politique de sécurité de l'information dans les relations avec les fournisseurs.....	28
15.1.2	La sécurité dans les accords conclus avec les fournisseurs.....	28
15.1.3	Chaîne d'approvisionnement informatique.....	29
15.2	Gestion de la prestation du service.....	29
16	Gestion des incidents liés à la sécurité de l'information.....	29
16.1	Gestion des incidents liés à la sécurité de l'information et améliorations.....	29
16.1.1	Responsabilités et procédures.....	29
16.1.2	Signalement des événements liés à la sécurité de l'information.....	29
16.1.3	Signalement des failles liées à la sécurité de l'information.....	29
16.1.4	Appréciation des événements liés à la sécurité de l'information et prise de décision.....	29
16.1.5	Réponse aux incidents liés à la sécurité de l'information.....	29
16.1.6	Tirer des enseignements des incidents liés à la sécurité de l'information.....	30
16.1.7	Recueil de preuves.....	30
17	Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité.....	30
17.1	Continuité de la sécurité de l'information.....	30
17.2	Redondances.....	30
17.2.1	Disponibilité des moyens de traitement de l'information.....	30
17.2.2	ENR – Communication d'urgence.....	30
18	Conformité.....	31

18.1	Conformité aux obligations légales et réglementaires	31
18.1.1	Identification de la législation et des exigences contractuelles applicables	31
18.1.2	Droits de propriété intellectuelle	32
18.1.3	Protection des enregistrements	32
18.1.4	Protection de la vie privée et protection des données à caractère personnel	32
18.1.5	Réglementation relative aux mesures cryptographiques	32
18.2	Revue de la sécurité de l'information	32
18.2.1	Revue indépendante de la sécurité de l'information	32
18.2.2	Conformité avec les politiques et les normes de sécurité	32
18.2.3	Examen de la conformité technique	32
Annexe A (normative) Objectifs de sécurité et mesures de sécurité de référence spécifiques à l'industrie des opérateurs de l'énergie		33
Bibliographie		37

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

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

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