
**Technologies de l'information —
Techniques de sécurité — Code de
bonnes pratiques pour la protection
des informations personnelles
identifiables (PII) dans l'informatique
en nuage public agissant comme
processeur de PII**

(<https://standards.iteh.ai/>)
*Information technology — Security techniques — Code of practice for
protection of personally identifiable information (PII) in public clouds
acting as PII processors*

ISO/IEC 27018:2019

<https://standards.iteh.ai/catalog/standards/iso/86300122-d81d-40e5-bde8-a8096b2fa1f5/iso-iec-27018-2019>



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

ISO/IEC 27018:2019

<https://standards.iteh.ai/catalog/standards/iso/86300122-d81d-40e5-bde8-a8096b2fa1f5/iso-iec-27018-2019>



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2019

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
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos	vi
Introduction	vii
1 Domaine d'application	1
2 Références normatives	1
3 Termes et définitions	1
4 Vue d'ensemble	3
4.1 Structure du présent document	3
4.2 Catégories de mesures	4
5 Politiques de sécurité de l'information	4
5.1 Orientations de la direction en matière de sécurité de l'information	4
5.1.1 Politiques de sécurité de l'information	5
5.1.2 Revue des 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	6
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
6.2 Appareils mobiles et télétravail	6
7 La sécurité des ressources humaines	6
7.1 Avant l'embauche	6
7.2 Pendant la durée du contrat	6
7.2.1 Responsabilités de la direction	6
7.2.2 Sensibilisation, apprentissage et formation à la sécurité de l'information	6
7.2.3 Processus disciplinaire	7
7.3 Rupture, terme ou modification du contrat de travail	7
8 Gestion des actifs	7
9 Contrôle d'accès	7
9.1 Exigences métier en matière de contrôle d'accès	7
9.2 Gestion de l'accès utilisateur	7
9.2.1 Enregistrement et désinscription des utilisateurs	7
9.2.2 Maîtrise de la gestion des accès utilisateur	7
9.2.3 Gestion des privilèges d'accès	8
9.2.4 Gestion des informations secrètes d'authentification des utilisateurs	8
9.2.5 Revue des droits d'accès utilisateur	8
9.2.6 Suppression ou adaptation des droits d'accès	8
9.3 Responsabilités des utilisateurs	8
9.3.1 Utilisation d'informations secrètes d'authentification	8
9.4 Contrôle de l'accès au système et aux applications	8
9.4.1 Restriction d'accès à l'information	8
9.4.2 Sécuriser les procédures de connexion	8
9.4.3 Système de gestion des mots de passe	8
9.4.4 Utilisation de programmes utilitaires à privilèges	9
9.4.5 Contrôle d'accès au code source des programmes	9
10 Cryptographie	9
10.1 Mesures cryptographiques	9
10.1.1 Politique d'utilisation des mesures cryptographiques	9
10.1.2 Gestion des clés	9
11 Sécurité physique et environnementale	9

11.1	Zones sécurisées.....	9
11.2	Équipement.....	9
11.2.1	Emplacement et protection du matériel.....	9
11.2.2	Services généraux.....	10
11.2.3	Sécurité du câblage.....	10
11.2.4	Maintenance du matériel.....	10
11.2.5	Sortie des actifs.....	10
11.2.6	Sécurité du matériel et des actifs hors des locaux.....	10
11.2.7	Mise au rebut ou recyclage sécurisé(e) du matériel.....	10
11.2.8	Matériel utilisateur laissé sans surveillance.....	10
11.2.9	Politique du bureau propre et de l'écran vide.....	10
12	Sécurité liée à l'exploitation.....	10
12.1	Procédures et responsabilités liées à l'exploitation.....	10
12.1.1	Procédures d'exploitation documentées.....	11
12.1.2	Gestion des changements.....	11
12.1.3	Dimensionnement.....	11
12.1.4	Séparation des environnements de développement, de test et d'exploitation.....	11
12.2	Protection contre les logiciels malveillants.....	11
12.3	Sauvegarde.....	11
12.3.1	Sauvegarde des informations.....	11
12.4	Journalisation et surveillance.....	12
12.4.1	Journalisation des événements.....	12
12.4.2	Protection de l'information journalisée.....	12
12.4.3	Journaux administrateur et opérateur.....	13
12.4.4	Synchronisation des horloges.....	13
12.5	Maîtrise des logiciels en exploitation.....	13
12.6	Gestion des vulnérabilités techniques.....	13
12.7	Considérations sur l'audit du système d'information.....	13
13	Sécurité des communications.....	13
13.1	Management de la sécurité des réseaux.....	13
13.2	Transfert de l'information.....	13
13.2.1	Politiques et procédures de transfert de l'information.....	13
13.2.2	Accords en matière de transfert d'information.....	14
13.2.3	Messagerie électronique.....	14
13.2.4	Engagements de confidentialité ou de non-divulgence.....	14
14	Acquisition, développement et maintenance des systèmes d'information.....	14
15	Relations avec les fournisseurs.....	14
16	Gestion des incidents liés à la sécurité de l'information.....	14
16.1	Gestion des incidents liés à la sécurité de l'information et améliorations.....	14
16.1.1	Responsabilités et procédures.....	14
16.1.2	Signalement des événements liés à la sécurité de l'information.....	15
16.1.3	Signalement des failles liées à la sécurité de l'information.....	15
16.1.4	Appréciation des événements liés à la sécurité de l'information et prise de décision.....	15
16.1.5	Réponse aux incidents liés à la sécurité de l'information.....	15
16.1.6	Tirer des enseignements des incidents liés à la sécurité de l'information.....	15
16.1.7	Recueil de preuves.....	15
17	Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité.....	15
18	Conformité.....	15
18.1	Conformité aux obligations légales et réglementaires.....	15
18.2	Revue de la sécurité de l'information.....	15
18.2.1	Revue indépendante de la sécurité de l'information.....	16
18.2.2	Conformité avec les politiques et les normes de sécurité.....	16
18.2.3	Examen de la conformité technique.....	16

Annexe A (normative) Ensemble étendu de mesures de protection des PII pour un processeur de PII d'un nuage public.....	17
Bibliographie.....	26

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

[ISO/IEC 27018:2019](https://standards.itih.ai/catalog/standards/iso/86300122-d81d-40e5-bde8-a8096b2fa1f5/iso-iec-27018-2019)

<https://standards.itih.ai/catalog/standards/iso/86300122-d81d-40e5-bde8-a8096b2fa1f5/iso-iec-27018-2019>