
**Techniques de sécurité — Extension
d'ISO/IEC 27001 et ISO/IEC 27002
au management de la protection de
la vie privée — Exigences et lignes
directrices**

*Security techniques — Extension to ISO/IEC 27001 and ISO/IEC
27002 for privacy information management — Requirements and
guidelines*



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.....	vii
Introduction.....	viii
1 Domaine d'application	1
2 Références normatives	1
3 Termes, définitions et abréviations	1
4 Généralités	2
4.1 Structure du présent document.....	2
4.2 Application des exigences de l'ISO/IEC 27001:2013.....	3
4.3 Application des lignes directrices de l'ISO/IEC 27002:2013.....	3
4.4 Client.....	4
5 Exigences spécifiques au PIMS liées à l'ISO/IEC 27001	4
5.1 Généralités.....	4
5.2 Contexte de l'organisation.....	4
5.2.1 Compréhension de l'organisation et de son contexte.....	4
5.2.2 Compréhension des besoins et des attentes des parties intéressées.....	5
5.2.3 Détermination du domaine d'application du système de management de la sécurité de l'information.....	5
5.2.4 Système de management de la sécurité de l'information.....	5
5.3 Leadership.....	6
5.3.1 Leadership et engagement.....	6
5.3.2 Politique.....	6
5.3.3 Rôles, responsabilités et autorités au sein de l'organisation.....	6
5.4 Planification.....	6
5.4.1 Actions face aux risques et opportunités.....	6
5.4.2 Objectifs de sécurité de l'information et plans pour les atteindre.....	7
5.5 Support.....	7
5.5.1 Ressources.....	7
5.5.2 Compétence.....	7
5.5.3 Sensibilisation.....	7
5.5.4 Communication.....	7
5.5.5 Informations documentées.....	8
5.6 Fonctionnement.....	8
5.6.1 Planification et contrôle opérationnels.....	8
5.6.2 Appréciation des risques de sécurité de l'information.....	8
5.6.3 Traitement des risques de sécurité de l'information.....	8
5.7 Évaluation des performances.....	8
5.7.1 Surveillance, mesures, analyse et évaluation.....	8
5.7.2 Audit interne.....	8
5.7.3 Revue de direction.....	8
5.8 Amélioration.....	9
5.8.1 Non-conformité et actions correctives.....	9
5.8.2 Amélioration continue.....	9
6 Recommandations spécifiques au PIMS liées à l'ISO/IEC 27002	9
6.1 Généralités.....	9
6.2 Politiques de sécurité de l'information.....	9
6.2.1 Orientations de la direction en matière de sécurité de l'information.....	9
6.3 Organisation de la sécurité de l'information.....	10
6.3.1 Organisation interne.....	10
6.3.2 Appareils mobiles et télétravail.....	11
6.4 La sécurité des ressources humaines.....	11
6.4.1 Avant l'embauche.....	11
6.4.2 Pendant la durée du contrat.....	11

6.4.3	Rupture, terme ou modification du contrat de travail.....	12
6.5	Gestion des actifs.....	12
6.5.1	Responsabilités relatives aux actifs.....	12
6.5.2	Classification de l'information.....	12
6.5.3	Manipulation des supports.....	13
6.6	Contrôle d'accès.....	14
6.6.1	Exigences métier en matière de contrôle d'accès.....	14
6.6.2	Gestion de l'accès utilisateur.....	14
6.6.3	Responsabilités des utilisateurs.....	16
6.6.4	Contrôle de l'accès au système et aux applications.....	16
6.7	Cryptographie.....	16
6.7.1	Mesures cryptographiques.....	16
6.8	Sécurité physique et environnementale.....	17
6.8.1	Zones sécurisées.....	17
6.8.2	Matériel.....	17
6.9	Sécurité liée à l'exploitation.....	19
6.9.1	Procédures et responsabilités liées à l'exploitation.....	19
6.9.2	Protection contre les logiciels malveillants.....	19
6.9.3	Sauvegarde.....	19
6.9.4	Journalisation et surveillance.....	20
6.9.5	Maîtrise des logiciels en exploitation.....	21
6.9.6	Gestion des vulnérabilités techniques.....	21
6.9.7	Considérations sur l'audit du système d'information.....	21
6.10	Sécurité des communications.....	22
6.10.1	Management de la sécurité des réseaux.....	22
6.10.2	Transfert de l'information.....	22
6.11	Acquisition, développement et maintenance des systèmes d'information.....	23
6.11.1	Exigences de sécurité applicables aux systèmes d'information.....	23
6.11.2	Sécurité des processus de développement et d'assistance technique.....	23
6.11.3	Données de test.....	25
6.12	Relations avec les fournisseurs.....	25
6.12.1	Sécurité de l'information dans les relations avec les fournisseurs.....	25
6.12.2	Gestion de la prestation du service.....	26
6.13	Gestion des incidents liés à la sécurité de l'information.....	26
6.13.1	Gestion des incidents liés à la sécurité de l'information et améliorations.....	26
6.14	Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité.....	29
6.14.1	Continuité de la sécurité de l'information.....	29
6.14.2	Redondances.....	29
6.15	Conformité.....	29
6.15.1	Conformité aux obligations légales et réglementaires.....	29
6.15.2	Revue de la sécurité de l'information.....	30

7	Recommandations supplémentaires de l'ISO/IEC 27002 pour les responsables de traitement de DCP.....	31
7.1	Généralités.....	31
7.2	Conditions de collecte et de traitement.....	31
7.2.1	Identifier et documenter la finalité.....	31
7.2.2	Identifier le fondement juridique.....	32
7.2.3	Déterminer quand et comment le consentement doit être obtenu.....	32
7.2.4	Obtenir et enregistrer le consentement.....	33
7.2.5	Étude de l'impact sur la vie privée.....	33
7.2.6	Contrats conclus avec les sous-traitants de DCP.....	34
7.2.7	Responsable conjoint de traitement.....	34
7.2.8	Enregistrements liés au traitement des DCP.....	35
7.3	Obligations vis-à-vis des personnes concernées.....	35
7.3.1	Identifier les obligations vis-à-vis des personnes concernées et y satisfaire.....	35
7.3.2	Déterminer les informations destinées aux personnes concernées.....	36
7.3.3	Fournir des informations aux personnes concernées.....	37
7.3.4	Fournir un mécanisme permettant de modifier ou de retirer le consentement.....	37

7.3.5	Fournir un mécanisme permettant de s'opposer au traitement des DCP	38
7.3.6	Accès, rectification et/ou suppression.....	38
7.3.7	Obligation d'information des tiers des responsables de traitement de DCP	39
7.3.8	Fourniture de copies des DCP traitées.....	39
7.3.9	Gestion des demandes.....	40
7.3.10	Prise de décision automatisée.....	40
7.4	Protection de la vie privée dès la conception et protection de la vie privée par défaut.....	40
7.4.1	Limiter la collecte.....	40
7.4.2	Limiter le traitement.....	41
7.4.3	Exactitude et qualité.....	41
7.4.4	Objectifs de minimisation des DCP	41
7.4.5	Dé-identification et suppression des DCP à la fin du traitement	42
7.4.6	Fichiers temporaires	42
7.4.7	Conservation	43
7.4.8	Mise au rebut.....	43
7.4.9	Mesures de transmission des DCP.....	43
7.5	Partage, transfert et divulgation des DCP	43
7.5.1	Identifier la base du transfert de DCP entre juridictions.....	44
7.5.2	Pays et organisations internationales auxquels les DCP peuvent être transférées.....	44
7.5.3	Enregistrements des transferts de DCP	44
7.5.4	Enregistrements de la divulgation de DCP à des tiers.....	45
8	Recommandations supplémentaires de l'ISO/IEC 27002 pour les sous-traitants de DCP ..	45
8.1	Généralités.....	45
8.2	Conditions de collecte et de traitement.....	45
8.2.1	Contrat client.....	45
8.2.2	Finalités de l'organisation.....	46
8.2.3	Utilisation à des fins de prospection et de publicité.....	46
8.2.4	Instruction en infraction.....	46
8.2.5	Obligations du client.....	47
8.2.6	Enregistrements liés au traitement des DCP	47
8.3	Obligations vis-à-vis des personnes concernées.....	47
8.3.1	Obligations vis-à-vis des personnes concernées.....	47
8.4	Protection de la vie privée dès la conception et protection de la vie privée par défaut.....	47
8.4.1	Fichiers temporaires.....	48
8.4.2	Restitution, transfert ou mise au rebut des DCP	48
8.4.3	Mesures de transmission des DCP.....	48
8.5	Partage, transfert et divulgation des DCP	49
8.5.1	Base du transfert de DCP entre juridictions.....	49
8.5.2	Pays et organisations internationales auxquels les DCP peuvent être transférées.....	49
8.5.3	Enregistrements de la divulgation de DCP à des tiers.....	50
8.5.4	Notification des demandes de divulgation de DCP	50
8.5.5	Divulgations de DCP juridiquement contraignantes.....	50
8.5.6	Divulgation des sous-traitants utilisés pour traiter des DCP	51
8.5.7	Recrutement d'un sous-traitant pour le traitement de DCP	51
8.5.8	Changement de sous-traitant pour le traitement de DCP	52
	Annexe A (normative) Objectifs et mesures de référence spécifiques au PIMS (responsables de traitement de DCP).....	53
	Annexe B (normative) Objectifs et mesures de référence spécifiques au PIMS (sous-traitants de DCP)	57
	Annexe C (informative) Correspondance avec l'ISO/IEC 29100.....	60
	Annexe D (informative) Correspondance avec le Règlement général sur la protection des données	63
	Annexe E (informative) Correspondance avec l'ISO/IEC 27018 et l'ISO/IEC 29151	66

Annexe F (informative) Comment appliquer l'ISO/IEC 27701 à l'ISO/IEC 27001 et l'ISO/IEC 27002.....	69
Bibliographie.....	71

Avant-propos

L'ISO (Organisation internationale de normalisation) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de l'IEC participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et l'IEC participent également aux travaux.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier de prendre note des différents critères d'approbation requis pour les différents types de document. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets) ou dans la liste des déclarations de brevets reçues par l'IEC (voir <https://patents.iec.c>).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir le lien suivant: www.iso.org/iso/fr/avant-propos.

Le présent document a été élaboré par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité*.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/fr/members.html.

Introduction

0.1 Généralités

Toutes les organisations ou presque traitent des données à caractère personnel (DCP). En outre, la quantité et les types de DCP traitées sont en augmentation, de même que le nombre de situations où une organisation a besoin de collaborer avec d'autres organisations en ce qui concerne le traitement des DCP. La protection de la vie privée dans le contexte du traitement des DCP est une nécessité sociétale, ainsi que l'objet de législations et/ou de réglementations dédiées dans le monde entier.

Le système de management de la sécurité de l'information (SMSI) défini dans l'ISO/IEC 27001 est conçu pour permettre l'ajout d'exigences spécifiques à des secteurs, sans qu'il soit nécessaire de concevoir un nouveau système de management. Les normes de l'ISO relatives aux systèmes de management, y compris celles qui sont spécifiques à des secteurs, sont conçues pour pouvoir être mises en œuvre séparément ou sous la forme d'un système de management combiné.

Les exigences et les recommandations relatives à la protection des DCP varient selon le contexte de l'organisation, particulièrement lorsqu'une législation et/ou des réglementations nationales existent. La norme ISO/IEC 27001 exige la compréhension et la prise en compte de ce contexte. Le présent document inclut une mise en correspondance avec:

- les principes et le cadre de la protection de la vie privée définis dans l'ISO/IEC 29100;
- l'ISO/IEC 27018;
- l'ISO/IEC 29151; et
- le Règlement général sur la protection des données.

Toutefois, il peut être nécessaire d'interpréter ces derniers afin de tenir compte de la législation et/ou de la réglementation locale.

Le présent document peut être utilisé par les responsables de traitement de DCP (y compris ceux qui sont des responsables conjoints de traitement) et les sous-traitants de DCP (y compris ceux qui utilisent des sous-traitants de DCP sous-traitants et ceux qui traitent des DCP en tant que sous-traitants à des sous-traitants de DCP).

Une organisation se conformant aux exigences du présent document produira des preuves documentaires de la façon dont elle gère le traitement des DCP. Ces preuves peuvent être utilisées pour faciliter les accords avec les partenaires d'affaires là où les deux parties sont concernées par le traitement des DCP. Cela peut également faciliter les relations avec d'autres parties prenantes. L'utilisation du présent document conjointement avec l'ISO/IEC 27001 peut, si cela est souhaité, permettre une vérification indépendante de ces preuves.

Le présent document a initialement été élaboré en tant que norme ISO/IEC 27552.

0.2 Compatibilité avec les autres normes de systèmes de management

Le présent document applique le cadre élaboré par l'ISO afin d'améliorer l'harmonisation entre ses normes de systèmes de management.

Le présent document permet à une organisation d'aligner ou d'intégrer son PIMS aux exigences d'autres normes de systèmes de management.