NORME INTERNATIONALE

ISO/IEC 27701

Première édition
2019-08

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

Numéro de référence
ISO/IEC 27701:2019(F)

DOCUMENT PROTÉGÉ PAR COPYRIGHT

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

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 règlementations 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 règlementations 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 règlementation 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.