NORME INTERNATIONALE

ISO/IEC 27018

Deuxième édition
2019-01

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

Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors



Numéro de référence
ISO/IEC 27018:2019(F)

© ISO/IEC 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**

© ISO/IEC 2019 – Tous droits réservés

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-divulgation ... 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

 © ISO/IEC 2019 – Tous droits réservés

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

Bibliographie **26**

© ISO/IEC 2019 – Tous droits réservés

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. Dans le domaine des technologies de l'information, l'ISO et l'IEC ont créé un comité technique mixte, l'ISO/IEC JTC 1.

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 documents ISO. 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).

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 ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*.

Cette seconde édition annule et remplace la première édition (ISO/IEC 27018:2014), dont elle constitue une révision mineure. La principale modification par rapport à l'édition précédente consiste en la correction d'une erreur rédactionnelle à l'Annexe A.

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.

© ISO/IEC 2019 – Tous droits réservés

Introduction

0.1 Historique et contexte

Les fournisseurs de services en nuage qui traitent des informations personnelles identifiables (PII, Personally Identifiable Information) dans le cadre d'un contrat avec leurs clients ont besoin de conduire leur prestation de services de manière à permettre aux deux parties de satisfaire aux exigences des lois et réglementations applicables en matière de protection des PII. Les exigences et les modalités de répartition des exigences entre le fournisseur de services en nuage et ses clients varient en fonction de la compétence juridique et selon les conditions du contrat établi entre le fournisseur de services en nuage et le client. La législation qui régit les modalités de traitement des PII (c'est-à-dire les modalités de collecte, d'utilisation, de transfert et de mise au rebut) est parfois appelée «législation en matière de protection des données); les PII sont parfois désignées comme «données à caractère personnel» ou «informations personnelles». Les obligations qui incombent à un processeur de PII varient d'une juridiction à l'autre, ce qui rend difficile pour les entreprises qui fournissent des services informatiques en nuage d'opérer dans plusieurs pays.

Un fournisseur de services en nuage public est un «processeur de PII» dès lors qu'il traite des PII pour un client de services en nuage et suivant les instructions de ce dernier. Le client de services en nuage, qui possède la relation contractuelle avec le processeur de PII du nuage public, peut être une personne physique, une «personne concernée», qui traite ses propres PII dans le nuage, un organisme ou un «contrôleur de PII», qui traite des PII en lien avec de nombreuses personnes concernées. Le client de services en nuage peut autoriser un ou plusieurs utilisateurs de services en nuage qui lui sont associés à utiliser les services mis à leur disposition dans le cadre de leur contrat avec le processeur de PII d'un nuage public. Noter que le client de services en nuage a autorité sur le traitement et l'utilisation des données. Un client de services en nuage qui agit également en tant que contrôleur de PII peut être soumis à un plus vaste ensemble d'obligations régissant la protection des PII que ne l'est le processeur de PII d'un nuage public. La distinction entre un contrôleur de PII et un processeur de PII repose sur le fait que le processeur de PII d'un nuage public n'a, en ce qui concerne le traitement des données, aucun objectif autre que ceux définis par le client de services en nuage pour ce qui a trait aux PII qu'il traite et aux opérations nécessaires pour atteindre les objectifs du client de services en nuages.

NOTE Lorsque le processeur de PII du nuage public traite des données de compte d'un client de services en nuage, il peut agir en qualité de contrôleur de PII à cette fin. Le présent document ne couvre pas cette activité.

L'intention du présent document, lorsqu'il est utilisé conjointement avec les objectifs et mesures de sécurité de l'information de l'ISO/IEC 27002, est de créer un ensemble commun de catégories et de mesures de sécurité pouvant être mis en œuvre par un fournisseur de services d'informatique en nuage public agissant en tant que processeur de PII. Ses objectifs sont les suivants:

— aider le fournisseur de services en nuage public à se conformer aux obligations applicables lorsqu'il agit en qualité de processeur de PII, que ces obligations incombent directement au processeur de PII ou qu'elles soient de nature contractuelle;

— permettre au processeur de PII d'un nuage public de faire preuve de transparence pour toute question pertinente de sorte que les clients de services en nuage puissent sélectionner des services de traitement des PII en nuage correctement gouvernés;

— assister le client de services en nuage et le processeur de PII d'un nuage public dans la conclusion d'un accord contractuel;

— fournir aux clients de services en nuage un mécanisme pour faire valoir les droits et responsabilités en matière d'audit et de conformité dans les cas où des audits de clients de services en nuage individuels portant sur des données hébergées dans un environnement de serveurs virtualisés («nuage») multipartie pourraient se révéler techniquement impossibles et pourraient amplifier les risques pour les mesures de sécurité réseau physiques et logiques en place.

Le présent document peut servir d'aide en fournissant un cadre de conformité commun pour les fournisseurs de services en nuage public, en particulier ceux qui interviennent sur un marché multinational.

© ISO/IEC 2019 – Tous droits réservés

0.2 Mesures de protection des PII pour les services d'informatique en nuage public

Le présent document est destiné à servir de référence pour permettre aux organismes de sélectionner des mesures de protection des PII dans le cadre du processus de mise en œuvre d'un système de management de la sécurité de l'information pour l'informatique en nuage selon l'ISO/IEC 27001, ou à servir de guide à l'attention d'organismes agissant en tant que processeurs de PII d'un nuage public pour la mise en œuvre de mesures de protection des PII largement reconnues. Le présent document a été plus particulièrement dérivé de l'ISO/IEC 27002, en tenant compte du ou des environnement(s) de risque spécifique(s) découlant des exigences en matière de protection des PII qui peuvent s'appliquer aux fournisseurs de services d'informatique en nuage public agissant en qualité de processeurs de PII.

En règle générale, un organisme qui met en œuvre l'ISO/IEC 27001 protège ses propres actifs informationnels. Cependant, dans le contexte des exigences de protection des PII applicables à un fournisseur de services en nuage public agissant en tant que processeur de PII, l'organisme protège les actifs informationnels qui lui sont confiés par ses clients. La mise en œuvre des mesures de l'ISO/IEC 27002 par le processeur de PII d'un nuage public à la fois convient à cette finalité et est nécessaire. Le présent document complète les mesures de l'ISO/IEC 27002 pour refléter la nature distribuée du risque et l'existence d'une relation contractuelle entre le client de services en nuage et le processeur de PII d'un nuage public. Le présent document complète l'ISO/IEC 27002 de deux manières:

— des préconisations de mise en œuvre applicables à la protection des PII dans l'informatique en nuage sont fournies pour certaines des mesures existantes de l'ISO/IEC 27002; et

— l'Annexe A fournit un ensemble de mesures supplémentaires et de recommandations associées visant à traiter les exigences en matière de protection des PII dans l'informatique en nuage public qui ne sont pas couvertes par l'ensemble de mesures existant de l'ISO/IEC 27002.

La plupart des mesures et recommandations du présent document s'appliquent également à un processeur de PII. Cependant, le contrôleur de PII est, dans la plupart des cas, soumis à des obligations supplémentaires qui ne sont pas spécifiées ici.

0.3 Exigences en matière de protection des PII

Il est essentiel qu'un organisme identifie ses exigences en matière de protection des PII. Ces exigences proviennent de trois sources principales, indiquées ci-dessous.

a) Exigences légales, statutaires, réglementaires et contractuelles: la première source comprend les exigences et obligations légales, statutaires, réglementaires et contractuelles qu'un organisme et ses partenaires commerciaux, contractants et prestataires de service, doivent satisfaire ainsi que leurs responsabilités socioculturelles et leur environnement opérationnel. Il convient de souligner le fait que les législations, réglementations et engagements contractuels faits par le processeur de PII peuvent imposer la sélection de mesures particulières et peuvent également nécessiter des critères spécifiques pour la mise en œuvre de ces mesures. Ces exigences peuvent varier d'une juridiction à une autre.

b) Risques: une autre source est dérivée de l'appréciation du risque propre à l'organisme en lien avec les PII, en prenant en compte la stratégie et les objectifs généraux de l'organisme. L'appréciation du risque permet d'identifier les menaces, d'analyser les vulnérabilités, de mesurer la vraisemblance des attaques et d'en évaluer l'impact potentiel. L'ISO/IEC 27005 fournit des recommandations pour la gestion du risque lié à la sécurité de l'information, comprenant des conseils sur l'appréciation des risques, l'acceptation des risques, la communication relative aux risques, la surveillance du risque et la révision du risque. L'ISO/IEC 29134 fournit des recommandations sur l'évaluation de l'impact sur la vie privée.

c) Politiques d'entreprise: bien que de nombreux aspects couverts par une politique d'entreprise découlent d'obligations légales et socioculturelles, un organisme peut volontairement choisir de dépasser les critères dérivés des exigences indiquées en a).

0.4 Sélection et mise en œuvre des mesures dans un environnement d'informatique en nuage

 © ISO/IEC 2019 – Tous droits réservés

Les mesures peuvent être sélectionnées en référence au présent document (qui inclut, par voie de référence, les mesures de l'ISO/IEC 27002, créant ainsi un ensemble de mesures de référence combinées pour le secteur ou l'application défini(e) dans le domaine d'application). Si besoin, des mesures peuvent être sélectionnées à partir d'autres ensembles de mesures, ou de nouvelles mesures peuvent être spécifiées en vue de satisfaire à des besoins spécifiques.

NOTE Un service de traitement de PII fourni par un processeur de PII d'un nuage public peut être considéré comme une application de l'informatique en nuage plutôt que comme un secteur en soi. Néanmoins, le terme «spécifique au secteur» est utilisé dans le présent document car il s'agit du terme conventionnel employé dans les autres normes de la série ISO/IEC 27000.

La sélection des mesures dépend des décisions prises par l'organisme en fonction de ses critères d'acceptation du risque, de ses options de traitement du risque et de l'approche de la gestion générale du risque appliquée à l'organisme et, en vertu des accords contractuels, à ses clients et fournisseurs. Elle est également soumise aux lois et réglementations nationales et internationales applicables. Lorsque les mesures du présent document ne sont pas sélectionnées, il y a lieu de l'indiquer en justifiant cette omission.

De plus, la sélection et la mise en œuvre des mesures dépend du rôle réel du fournisseur de services en nuage public dans le contexte de l'architecture de référence globale de l'informatique en nuage (voir l'ISO/IEC 17789). De nombreux organismes différents peuvent être impliqués dans la fourniture de services d'infrastructure et d'application dans un environnement d'informatique en nuage. Dans certaines circonstances, les mesures sélectionnées peuvent être spécifiques à une catégorie de service particulière de l'architecture de référence de l'informatique en nuage. Dans d'autres cas, il peut y avoir des rôles partagés dans la mise en œuvre des mesures de sécurité. Il est nécessaire que les accords contractuels spécifient clairement les responsabilités en matière de protection des PII de tous les organismes impliqués dans la fourniture ou l'utilisation de services en nuage, y compris le processeur de PII d'un nuage public, ses sous-traitants et le client de services en nuage.

Les mesures du présent document peuvent être considérées comme des principes directeurs et être appliquées à la plupart des organismes. Elles sont expliquées plus en détail ci-dessous, avec des préconisations de mise en œuvre. La mise en œuvre peut être simplifiée si les exigences applicables à la protection des PII ont été prises en compte dans la conception du système d'information, des services et des opérations du processeur de PII d'un nuage public. Cette prise en compte est un élément du concept souvent appelé «respect de la vie privée dès la conception» (voir l'article bibliographique [9]).

0.5 Élaboration de lignes directrices supplémentaires

Le présent document peut servir de base pour la mise au point de lignes directrices applicables à la protection des PII. Il est possible qu'une partie des mesures et recommandations de ce code de bonnes pratiques ne soit pas applicable. Par ailleurs, des mesures et des lignes directrices supplémentaires ne figurant pas dans le présent document peuvent être nécessaires. Lors de la rédaction de documents contenant des lignes directrices ou des mesures supplémentaires, il peut être utile d'intégrer des références croisées aux articles du présent document, le cas échéant, afin de faciliter la vérification de la conformité par les auditeurs et les partenaires commerciaux.

0.6 Examen du cycle de vie

Les PII sont soumises à un cycle de vie naturel, depuis leur création et leur origine en passant par leur stockage, leur traitement, leur utilisation, leur transmission, jusqu'à leur destruction finale ou leur obsolescence. Les risques pour les PII peuvent varier pendant leur durée de vie, mais la protection des PII demeure importante dans une certaine mesure à toutes les phases du cycle.

Il est nécessaire de prendre en compte les exigences applicables à la protection des PII étant donné que les systèmes d'information, nouveaux ou existants, sont gérés tout au long de leur cycle de vie.

© ISO/IEC 2019 – Tous droits réservés

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

1 Domaine d'application

Le présent document établit des objectifs de sécurité communément acceptés, des mesures de sécurité et des lignes directrices de mise en œuvre de mesures destinées à protéger les informations personnelles identifiables (PII) conformément aux principes de protection de la vie privée de l'ISO/IEC 29100 pour l'environnement informatique en nuage public.

En particulier, le présent document spécifie des lignes directrices dérivées de l'ISO/IEC 27002, en tenant compte des exigences réglementaires relatives à la protection des PII, qui peuvent être applicables dans le contexte du ou des environnements de risque liés à la sécurité de l'information d'un fournisseur de services en nuage public.

Le présent document s'applique aux organismes de tous types et de toutes tailles, y compris les sociétés publiques et privées, les entités gouvernementales et les organismes à but non lucratif, qui offrent des services de traitement de l'information en tant que processeurs de PII via l'informatique en nuage sous contrat auprès d'autres organismes.

Les lignes directrices du présent document peuvent également s'appliquer aux organismes agissant en tant que contrôleurs de PII. Cependant, les contrôleurs de PII peuvent être soumis à d'autres lois, réglementations et obligations en matière de protection des PII qui ne s'appliquent pas aux processeurs de PII. Le présent document n'a pas pour objet de couvrir des obligations supplémentaires.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO/IEC 17788, *Technologies de l'information — Informatique en nuage — Vue d'ensemble et vocabulaire*

ISO/IEC 27000, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*

ISO/IEC 27002:2013, *Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO/IEC 17788, et l'ISO/IEC 27000 ainsi que les suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

— ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

© ISO/IEC 2019 – Tous droits réservés