NORME INTERNATIONALE

ISO/IEC 27017

Première édition
2015-12-15

Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage

Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Numéro de référence
ISO/IEC 27017:2015(F)

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 (Organization internationale de normalization) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalization 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'organization 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 Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/IEC, Partie 2.

La tâche principale du comité technique mixte est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des organismes nationaux votants.

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.

L'ISO/IEC 27017 a été élaborée par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*, en collaboration avec l'UIT-T. Le même texte est publié en tant que recommandation UIT-T. X.1631 (07/2015).

Introduction

Les lignes directrices contenues dans la présente Recommandation | Norme internationale viennent à l'appui et en complément des lignes directrices données dans l'ISO/IEC 27002.

Spécifiquement, cette Recommandation | Norme internationale fournit des lignes directrices appuyant la mise en œuvre des mesures de sécurité de l'information pour les clients et les fournisseurs de services en nuage. Certaines lignes directrices sont destinées aux clients des services du nuage qui ensurent la mise en œuvre des mesures, tandis que d'autres sont destinées aux fournisseurs de services en nuage afin de soutenir la mise en œuvre de ces mesures. Le choix approprié des mesures de sécurité de l'information et l'application des recommandations de mise en œuvre fournies dépendra d'une appréciation du risque et de toute exigence légale, contractuelle, réglementaire ou autre en matière de sécurité de l'information spécifique au secteur du nuage.

Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage

1 Domaine d'application

La présente Recommandation | Norme internationale contient des lignes directrices relatives aux mesures de sécurité de l'information applicables à la prestation et à l'utilization de services d'informatique en nuage, par exemple:

— des recommandations supplémentaires concernant la mise en œuvre des mesures de sécurité pertinentes spécifiées dans l'ISO/IEC 27002;

— des mesures de sécurité supplémentaires avec préconisations de mise en œuvre spécifiquement liées aux services en nuage.

La présente Recommandation | Norme internationale fournit des recommandations concernant les moyens de maîtrise et la mise en œuvre destinées aux prestataires de services d'informatique en nuage et à leurs clients.

2 Références normatives

Les Recommandations et Normes internationales suivantes contiennent des dispositions qui, par suite de la référence qui en est faite, constituent des dispositions valables pour la présente Recommandation | Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes les Recommandations | Normes internationales sont sujettes à révision et les parties prenantes des accords fondés sur la présente Recommandation | Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et Normes indiquées ci-après. Les membres de l'IEC et de l'ISO possèdent le registre des Normes Internationales en vigueur à un moment donné. Le Bureau de la normalization des télécommunications de l´UIT tient à jour une liste des Recommandations de l´UIT-T en vigueur.

RECOMMANDATION UIT-T Y 3500 (en vigueur) | ISO/IEC 17788: (en vigueur), *Technologies de l'information — Informatique en nuage — Vue d'ensemble et vocabulaire*

RECOMMANDATION UIT-T Y 3502 (en vigueur) | ISO/IEC 17789: (en vigueur), *Technologies de l'information — Informatique en nuage — Architecture de référence*

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, définitions et abréviations

3.1 Termes et définitions

Pour les besoins de la présente Recommandation | Norme internationale, les termes et définitions de l'ISO/IEC 27000, la Rec. UIT-T Y.3500 | l'ISO/IEC 17788, la Rec. UIT-T Y.3502 | l'ISO/IEC 17789 ainsi que les suivants, s'appliquent:

3.1.1
aptitude
qualité d'être capable d'accomplir une activité donnée.

3.1.2
violation de données
compromission de sécurité qui entraîne la destruction accidentelle ou illégale, la perte, l'altération, la divulgation non autorisée ou l'accès à des données protégées transmises, stockées, ou soumises à un quelconque autre traitement;**multilocation sécurisée:** type de multilocation qui emploie des contrôles de sécurité pour une protection explicite contre les violations de données et qui produit la validation de ces contrôles pour une bonne gouvernance.

Note 1 à l'article: La multilocation sécurisée existe lorsque le profil de risque d'un locataire individuel n'est pas plus important qu'il ne le serait dans un environnement dédié à un seul locataire.

Note 2 à l'article: Dans les environnements très sécurisés, même l'identité des locataires est tenue secrète.

3.1.3
machine virtuelle
l'environnement complet qui supporte l'exécution des logiciels invités.

Note 1 à l'article: Une machine virtuelle est une encapsulation complète du matériel virtuel, des disques virtuels et des métadonnées qui y sont associées. Les machines virtuelles permettent le multiplexage de la machine physique sous-jacente par le biais d'une couche logicielle appelée hyperviseur.

3.2 Abréviations

Pour les besoins de la présente Recommandation | Norme internationale, les abréviations suivantes s'appliquent.

DCP	Données à caractère personnel
IaaS	Infrastructure en tant que service (Infrastructure as a Service)
MV	machine virtuelle
PaaS	Plate-forme en tant que service (Platform as a Service)
SaaS	Logiciel en tant que service (Software as a Service)
SLA	Accord de niveau de service (Service Level Agreement)

4 Concepts spécifiques au secteur du nuage

4.1 Vue d'ensemble

L'utilization de l'informatique en nuage a modifié la façon dont il convient que les organismes apprécient et atténuent les risques liés à la sécurité de l'information en raison des changements importants dans la manière dont les ressources informatiques sont techniquement conçues, exploitées et gérées. La présente Recommandation | Norme internationale fournit des lignes directrices supplémentaires pour la mise en œuvre spécifique au nuage, fondées sur l'ISO/IEC 27002, et prévoit des mesures supplémentaires visant à traiter les considérations spécifiques au nuage en matière de menaces et les risques de sécurité des informations.

Il convient que les utilizateurs de la présente Recommandation | Norme internationale se réfèrent aux Articles 5 à 18 de l'ISO/IEC 27002 concernant les mesures, les préconisations de mise en œuvre et autres informations. En raison de l'applicabilité générale de l'ISO/IEC 27002, de nombreuses mesures, préconisations de mise en œuvre et autres informations s'appliquent à la fois au contexte général et au contexte de l'informatique en nuage d'un organisme. Par exemple, «6.1.2 Séparation des tâches» de

l'ISO/IEC 27002 prévoit une mesure qui peut être appliquée, que l'organisme agisse ou non en tant que fournisseur de services en nuage. Un client de services en nuage peut en outre tirer de la même mesure des exigences de séparation des tâches dans l'environnement du nuage, par exemple en séparant les administrateurs et les utilizateurs des services en nuage pour les clients de ces services.

En tant que complément à l'ISO/IEC 27002, la présente Recommandation | Norme internationale fournit en outre des mesures spécifiques aux services en nuage, des préconisations de mise en œuvre et d'autres informations (voir paragraphe 4.5) destinées à atténuer les risques qui accompagnent les caractéristiques techniques et opérationnelles des services en nuage (voir l'Annexe B). Les clients et les fournisseurs des services en nuage peuvent se référer à l'ISO/IEC 27002 ainsi qu'à la présente Recommandation | Norme internationale pour choisir les mesures appropriées à l'aide des préconisations de mise en œuvre et ajouter d'autres mesures si nécessaire. Ce processus peut être réalisé en effectuant une appréciation et un traitement du risque en matière de sécurité des informations dans le contexte organisationnel et opérationnel où les services en nuage sont utilizés ou fournis (voir paragraphe 4.4).

4.2 Relations avec les fournisseurs dans les services en nuage

L'Article 15 de l'ISO/IEC 27002 «Relations avec les fournisseurs» fournit des mesures, des préconisations de mise en œuvre et d'autres informations pour la gestion de la sécurité de l'information dans les relations avec les fournisseurs. La prestation et l'utilization de services en nuage est un type de relation avec les fournisseurs où le client des services en nuage est un acquéreur, et le fournisseur des services en nuage est un fournisseur. L'article s'applique donc aux clients et aux fournisseurs de services en nuage.

Les clients et les fournisseurs de services en nuage peuvent également former une chaîne d'approvisionnement. Supposons qu'un prestataire de services en nuage fournisse un service de type aptitudes d'infrastructure. En outre, un autre fournisseur de services en nuage peut fournir un service de type aptitudes d'application. Dans ce cas, le second fournisseur de services en nuage est un client du premier et un fournisseur de services en nuage pour le client qui utilize ses services. Cet exemple illustre le cas où la présente Recommandation | Norme internationale s'applique à un organisme à la fois en tant que client de services en nuage et en tant que fournisseur de services en nuage. Comme les clients et les fournisseurs de services en nuage forment une chaîne d'approvisionnement du fait de la conception et de la mise en œuvre du ou des services en nuage, le paragraphe 15.1.3 «Chaîne d'approvisionnement informatique» de l'ISO/IEC 27002 s'applique.

La Norme internationale en plusieurs parties ISO/IEC 27036, «*Sécurité d'information pour la relation avec le fournisseur*», fournit à l'acquéreur et au fournisseur de produits et de services des recommandations détaillées concernant la sécurité de l'information dans les relations avec les fournisseurs.

La partie 4 de l'ISO/IEC 27036 traite directement de la sécurité des services en nuage dans les relations avec les fournisseurs. Cette norme s'applique également aux clients des services en nuage en tant qu'acquéreurs et aux prestataires de services en nuage en tant que fournisseurs.

4.3 Relations entre les clients de services en nuage et les fournisseurs de services en nuage

Dans l'environnement de l'informatique en nuage, les données des clients des services sont stockées, transmises et traitées par un service en nuage. Par conséquent, les processus métier d'un client de service en nuage peuvent dépendre de la sécurité des informations du service en nuage. Sans un contrôle suffisant sur le service en nuage, le client du service peut avoir à prendre des précautions supplémentaires concernant ses pratiques en matière de sécurité de l'information.

Avant d'entrer en relation avec un fournisseur, le client du service en nuage doit choisir un service, en tenant compte des écarts possibles entre les exigences en matière de sécurité de l'information du client du service en nuage et les aptitudes du service en matière de sécurité de l'information. Une fois qu'un service en nuage est sélectionné, il convient que le client gère l'utilization du service en nuage de sorte à répondre à ses exigences en matière de sécurité de l'information. Dans cette relation, il convient que le fournisseur de services en nuage fournisse les informations et l'assistance technique nécessaires pour répondre aux exigences du client du service en nuage en matière de sécurité de l'information. Lorsque les mesures de sécurité de l'information fournies par le fournisseur de services en nuage sont

prédéfinies et ne peuvent pas être modifiées par le client du service en nuage, ce dernier peut également avoir besoin de mettre en œuvre certaines de ses propres mesures afin d'atténuer les risques.

4.4 Gestion des risques relatifs à la sécurité de l'information dans les services en nuage

Il convient que les clients et les fournisseurs de services en nuage disposent de processus de gestion des risques liés à la sécurité de l'information. Il est conseillé qu'ils se réfèrent à l'ISO/IEC 27001 pour les exigences relatives à la gestion des risques dans leurs systèmes de gestion de la sécurité de l'information, et à l'ISO/IEC 27005 pour des préconisations supplémentaires concernant la gestion des risques de sécurité de l'information en elle-même. L'ISO 31000, à laquelle l'ISO/IEC 27001 et l'ISO/IEC 27005 se conforment, peut également contribuer à la compréhension générale de la gestion des risques.

Contrairement à l'applicabilité générale des processus de gestion des risques liés à la sécurité de l'information, l'informatique en nuage a ses propres types de sources de risques, y compris les menaces et les vulnérabilités, qui découlent de ses caractéristiques. Par exemple, la mise en réseau, l'extensibilité et l'adaptabilité du système, le partage des ressources, la fourniture de libre-service, l'administration à la demande, la fourniture de services inter-juridictionnels et la visibilité limitée de la mise en œuvre des mesures. L'Annexe B fournit des références qui donnent des informations sur ces sources de risques et sur les risques associés à la prestation et à l'utilization des services en nuage.

Les mesures et les préconisations de mise en œuvre données dans les Articles 5 à 18 et dans l'Annexe A de la présente Recommandation | Norme internationale traitent des sources de risques et des risques spécifiques à l'informatique en nuage.

4.5 Structure de la présente norme

La présente Recommandation | Norme internationale est structurée dans un format similaire à celui de l'ISO/IEC 27002. La présente Recommandation | Norme internationale inclut les Articles 5 à 18 de l'ISO/IEC 27002 en précisant l'applicabilité de ses textes à chaque article et paragraphe.

Lorsque les objectifs et mesures spécifiés dans l'ISO/IEC 27002 sont applicables sans nécessiter d'informations supplémentaires, seule une référence à l'ISO/IEC 27002 est fournie.

Lorsqu'un objectif accompagné de mesures, ou une mesure sous un objectif de l'ISO/IEC 27002, est nécessaire en plus de ceux de l'ISO/IEC 27002, ceux-ci sont indiqués à l'Annexe A normative: Ensemble étendu de mesures pour les services en nuage. Lorsqu'une mesure de l'ISO/IEC 27002 ou de l'Annexe A de la présente Recommandation | Norme internationale nécessite une préconisation de mise en œuvre supplémentaire spécifique aux services en nuage concernant la mesure, elle est fournie sous le sous-titre «**Préconisation de mise en œuvre pour les services en nuage**». La préconisation est donnée selon l'un des deux types suivants:

Le type 1 est utilizé en cas de préconisation séparée pour le client et le fournisseur de services en nuage.

Le type 2 est utilizé si la préconisation est la même pour le client et pour le fournisseur de services en nuage.

Type 1

Client de services en nuage	Fournisseur de services en nuage

Type 2

Client de services en nuage	Fournisseur de services en nuage

Des informations supplémentaires dont la prise en compte peut être nécessaire sont fournies sous le sous-titre «**Autres informations pour les services en nuage**».

5 Politiques de sécurité de l'information

5.1 Orientations de la direction en matière de sécurité de l'information

L'objectif spécifié au paragraphe 5.1 de l'ISO/IEC 27002 s'applique.

5.1.1 Politiques de sécurité de l'information

La mesure 5.1.1 et les préconisations de mise en œuvre et autres informations associées spécifiées dans l'ISO/IEC 27002 s'appliquent. Les préconisations suivantes spécifiques au secteur s'appliquent également.

Préconisation de mise en œuvre pour les services en nuage

Client de services en nuage	Fournisseur de services en nuage
Il convient de définir une politique de sécurité des informations pour l'informatique en nuage en tant que politique portant sur le thème spécifique du client de services en nuage. En ce qui concerne l'informatique en nuage, il convient que la politique de sécurité de l'information du client des services en nuage soit cohérente avec les niveaux acceptables de risques liés à la sécurité de l'information définis par l'organisme pour ses informations et autres actifs. Lors de la définition de la politique de sécurité des informations pour l'informatique en nuage, il convient que le client de services en nuage tienne compte des éléments suivants: — les informations stockées dans l'environnement informatique en nuage peuvent être soumises à l'accès et à la gestion par le fournisseur de services en nuage; — les actifs peuvent être maintenus dans l'environnement informatique en nuage, par exemple applications, programmes; — les processus peuvent être utilisés sur un service en nuage virtualisé, en multilocation; — les utilisateurs du service en nuage et le contexte dans lequel ils utilisent le service en nuage; — les administrateurs du service en nuage du client de services en nuage qui disposent de privilèges d'accès; — les emplacements géographiques de l'organisme du fournisseur de services en nuage et les pays où celui-ci peut stocker les données du client de services en nuage (y compris de manière temporaire).	Il convient que le fournisseur de services en nuage renforce sa politique de sécurité de l'information afin de traiter la fourniture et l'utilisation de ses services en nuage, en tenant compte des éléments suivants: — les exigences de référence en matière de sécurité de l'information applicables à la conception et à la mise en œuvre du service en nuage; — les risques liés aux internes autorisés; — la multilocation et l'isolement des clients des services en nuage (y compris la virtualisation); — l'accès aux actifs du client de services en nuage par le personnel du fournisseur de services en nuage; — les procédures de contrôle d'accès, par exemple authentification stricte pour l'accès administratif aux services en nuage; — la communication avec les clients des services en nuage pendant la gestion des changements; — la sécurité de la virtualisation; — l'accès aux données des clients des services en nuage et leur protection; — la gestion du cycle de vie des comptes des clients des services en nuage; — la communication des violations et des lignes directrices en matière de partage d'informations afin de faciliter les enquêtes et la criminalistique.

Autres informations pour les services en nuage

En matière d'informatique en nuage, la politique de sécurité des informations du client des services en nuage est l'une des politiques portant sur des thèmes spécifiques décrites dans l'ISO/IEC 27002 5.1.1. La politique de sécurité de l'information d'un organisme porte sur ses informations et ses processus métier. Lorsqu'un organisme utilize des services dans les nuages, il peut avoir une politique pour l'informatique en nuage en tant que client de services en nuage. Les informations d'un organisme peuvent être stockées et maintenues dans l'environnement informatique en nuage, et les processus métier peuvent être exploités dans l'environnement informatique en nuage. Les exigences générales en matière de sécurité de l'information définies dans la politique de sécurité de l'information au niveau supérieur sont suivies par la politique pour l'informatique en nuage.

En revanche, la politique de sécurité de l'information pour la fourniture des services en nuage traite des informations et des processus métier des clients des services en nuage, et non des informations et des processus métier du fournisseur de services en nuage. Il convient que les exigences en matière de sécurité de l'information pour la fourniture de services en nuage répondent à celles des clients potentiels de services en nuage. Par conséquent, elles peuvent ne pas être cohérentes avec les exigences en matière de sécurité de l'information et de processus métier du fournisseur de services en nuage. Le domaine d'application de la politique de sécurité de l'information est souvent défini en termes de service, mais pas seulement par la structure organisationnelle ou les emplacements physiques.

Il existe plusieurs aspects de sécurité en matière de virtualisation pour l'informatique en nuage, notamment la gestion du cycle de vie des instances virtuelles, le stockage et les contrôles d'accès aux images virtualisées, la gestion des instances virtuelles dormantes ou hors ligne, les instantanés, la protection des hyperviseurs et les mesures de sécurité régissant l'utilization des portails en libre-service.

5.1.2 Revue des politiques de sécurité de l'information

La mesure 5.1.2 et les préconisations de mise en œuvre et autres informations associées spécifiées dans l'ISO/IEC 27002 s'appliquent.

6 Organization de la sécurité de l'information

6.1 Organization interne

L'objectif spécifié au paragraphe 6.1 de l'ISO/IEC 27002 s'applique.

6.1.1 Fonctions et responsabilités liées à la sécurité de l'information

La mesure 6.1.1 et les préconisations de mise en œuvre et autres informations associées spécifiées dans l'ISO/IEC 27002 s'appliquent. Les préconisations suivantes spécifiques au secteur s'appliquent également.

Préconisation de mise en œuvre pour les services en nuage

Client de services en nuage	Fournisseur de services en nuage
Il convient que le client de services en nuage convienne avec le fournisseur de services en nuage d'une répartition appropriée des rôles et responsabilités en matière de sécurité de l'information, et qu'il confirme sa capacité à remplir les rôles et responsabilités qui lui sont attribués. Il convient de définir dans un accord les rôles et responsabilités des deux parties en matière de sécurité de l'information. Il convient que le client de services en nuage identifie et gère sa relation avec la fonction de support et d'aide au client du fournisseur de services en nuage.	Il convient que le fournisseur de services en nuage accepte et documente une répartition appropriée des rôles et responsabilités en matière de sécurité de l'information avec ses clients de services en nuage, ses prestataires de services en nuage et ses fournisseurs.

Autres informations pour les services en nuage

Même lorsque les responsabilités sont déterminées au sein des parties et entre elles, le client de services en nuage est responsable de la décision d'utilizer le service. Il convient que cette décision soit prise en fonction des rôles et des responsabilités déterminés au sein de l'organisme du client de services en nuage. Le fournisseur de services en nuage est responsable de la sécurité de l'information prévue dans le cadre du contrat de services en nuage. Il convient d'effectuer la mise en œuvre et la fourniture de la sécurité de l'information conformément aux rôles et responsabilités déterminés au sein de l'organisme du fournisseur de services en nuage.

Toute ambiguïté dans les rôles et dans la définition et l'attribution des responsabilités liées à des questions telles que la propriété des données, le contrôle d'accès et la maintenance des infrastructures, peut donner lieu à des litiges commerciaux ou juridiques, notamment en cas de rapports avec des tiers.

Les données et les fichiers sur les systèmes du fournisseur de services en nuage créés ou modifiés pendant l'utilization du service en nuage peuvent avoir une importance critique pour le fonctionnement sécurisé, la récupération et la continuité du service. Il convient de définir et de documenter la propriété de tous les actifs ainsi que les parties ayant des responsabilités concernant les opérations associées à ces actifs, par exemple les opérations de sauvegarde et de récupération. Dans le cas contraire, il existe un risque que le fournisseur de services en nuage suppose que le client de services en nuage ensure la réalisation de ces tâches vitales (ou inversement), et une perte de données peut avoir lieu.

6.1.2 Séparation des tâches

La mesure 6.1.2 et les préconisations de mise en œuvre et autres informations associées spécifiées dans l'ISO/IEC 27002 s'appliquent.

6.1.3 Relations avec les autorités

La mesure 6.1.3 et les préconisations de mise en œuvre et autres informations associées spécifiées dans l'ISO/IEC 27002 s'appliquent. Les préconisations suivantes spécifiques au secteur s'appliquent également.

Préconisation de mise en œuvre pour les services en nuage

Client de services en nuage	Fournisseur de services en nuage
Il convient que le client de services en nuage identifie les autorités compétentes pour une exploitation combinée du client et du fournisseur de services en nuage.	Il convient que le fournisseur de services en nuage informe le client des emplacements géographiques de l'organisme du fournisseur de services en nuage et des pays où le fournisseur de services en nuage peut stocker les données du client de services en nuage.

Autres informations pour les services en nuage

Les informations relatives aux emplacements géographiques où les données du client de services en nuage peuvent être stockées ou transmises peuvent aider le client de services en nuage à déterminer les autorités de contrôle et les juridictions.

6.1.4 Relations avec des groupes de travail spécialisés

La mesure 6.1.4 et les préconisations de mise en œuvre et autres informations associées spécifiées dans l'ISO/IEC 27002 s'appliquent.

6.1.5 La sécurité de l'information dans la gestion de projet

La mesure 6.1.5 et les préconisations de mise en œuvre et autres informations associées spécifiées dans l'ISO/IEC 27002 s'appliquent.

6.2 Appareils mobiles et télétravail

L'objectif spécifié au paragraphe 6.2 de l'ISO/IEC 27002 s'applique.

6.2.1 Politique en matière d'appareils mobiles

La mesure 6.2.1 et les préconisations de mise en œuvre et autres informations associées spécifiées dans l'ISO/IEC 27002 s'appliquent.