
**Technologies de l'information —
Techniques de sécurité — Code de
bonne pratique pour le management
de la sécurité de l'information**

*Information technology — Security techniques — Code of practice for
information security controls*



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/CEI 2013

Droits de reproduction réservés. Sauf indication contraire, 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, l'affichage sur l'internet ou sur un Intranet, sans autorisation écrite préalable. Les demandes d'autorisation peuvent être adressées 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 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos.....	v
0 Introduction.....	vi
1 Domaine d'application.....	1
2 Références normatives.....	1
3 Termes et définitions.....	1
4 Structure de la présente norme.....	1
4.1 Articles.....	1
4.2 Catégories de mesures.....	2
5 Politiques de sécurité de l'information.....	2
5.1 Orientations de la direction en matière de sécurité de l'information.....	2
6 Organisation de la sécurité de l'information.....	4
6.1 Organisation interne.....	4
6.2 Appareils mobiles et télétravail.....	7
7 La sécurité des ressources humaines.....	9
7.1 Avant l'embauche.....	9
7.2 Pendant la durée du contrat.....	11
7.3 Rupture, terme ou modification du contrat de travail.....	14
8 Gestion des actifs.....	15
8.1 Responsabilités relatives aux actifs.....	15
8.2 Classification de l'information.....	16
8.3 Manipulation des supports.....	19
9 Contrôle d'accès.....	21
9.1 Exigences métier en matière de contrôle d'accès.....	21
9.2 Gestion de l'accès utilisateur.....	23
9.3 Responsabilités des utilisateurs.....	27
9.4 Contrôle de l'accès au système et aux applications.....	28
10 Cryptographie.....	31
10.1 Mesures cryptographiques.....	31
11 Sécurité physique et environnementale.....	34
11.1 Zones sécurisées.....	34
11.2 Matériels.....	37
12 Sécurité liée à l'exploitation.....	42
12.1 Procédures et responsabilités liées à l'exploitation.....	42
12.2 Protection contre les logiciels malveillants.....	46
12.3 Sauvegarde.....	47
12.4 Journalisation et surveillance.....	48
12.5 Maîtrise des logiciels en exploitation.....	50
12.6 Gestion des vulnérabilités techniques.....	51
12.7 Considérations sur l'audit du système d'information.....	53
13 Sécurité des communications.....	54
13.1 Management de la sécurité des réseaux.....	54
13.2 Transfert de l'information.....	56
14 Acquisition, développement et maintenance des systèmes d'information.....	60
14.1 Exigences de sécurité applicables aux systèmes d'information.....	60
14.2 Sécurité des processus de développement et d'assistance technique.....	63
14.3 Données de test.....	68
15 Relations avec les fournisseurs.....	69
15.1 Sécurité de l'information dans les relations avec les fournisseurs.....	69