



Norme de sécurité des données de l'industrie des cartes de paiement

Établir et maintenir un réseau sécuritaire

- Exigence 1 : Installer et maintenir une configuration de pare-feu pour protéger les données.
- Exigence 2 : Ne pas utiliser les paramètres par défaut du fournisseur dans le cas des mots de passe et des autres paramètres de sécurité.

Protéger les données des titulaires de carte

- Exigence 3 : Protéger les données conservées.
- Exigence 4 : Chiffrer la transmission des données des titulaires de carte et de l'information de nature délicate par le biais des réseaux publics.

Maintenir un programme de gestion de la vulnérabilité

- Exigence 5 : Utiliser et mettre régulièrement à jour un logiciel d'anti-virus.
- Exigence 6 : Développer et maintenir des systèmes et des applications sécuritaires.

Mettre en place de solides mesures de contrôle de l'accès

- Exigence 7 : Restreindre l'accès aux données aux personnes qui ont besoin de les connaître.
- Exigence 8 : Attribuer un code d'utilisateur unique à chaque personne ayant accès à l'ordinateur.
- Exigence 9 : Restreindre l'accès physique aux données des titulaires de carte.

Surveiller et tester régulièrement les réseaux

- Exigence 10 : Assurer un suivi et une surveillance de tout accès aux ressources du réseau et aux données des titulaires de carte.
- Exigence 11 : Tester régulièrement les systèmes et les processus de sécurité.

Maintenir une politique de sécurité de l'information

- Exigence 12 : Maintenir une politique en matière de sécurité de l'information.

Cette norme s'applique aux membres de Visa, aux marchands et aux fournisseurs de services qui conservent, traitent ou transmettent des données sur les titulaires de carte. De plus, des exigences de sécurité s'appliquent à toutes les « composantes informatiques », soit les composantes d'un réseau, les serveurs et les applications reliés à l'environnement des données des titulaires de carte. Les composantes d'un réseau comprennent, entre autres, les pare-feu, les commutateurs, les routeurs, les points d'accès sans fil, les appareils du réseau et les autres appareils de sécurité. Les serveurs comprennent, entre autres, le Web, les bases de données, l'authentification, le DNS, le

courrier, les serveurs proxy et les serveurs de temps NTP. Les applications comprennent toutes les applications achetées ou personnalisées, y compris les applications internes et externes (Web).

Établir et maintenir un réseau sécuritaire

Exigence 1 : Installer et maintenir une configuration de pare-feu pour protéger les données.

Les pare-feu sont des appareils informatiques qui contrôlent le trafic informatique autorisé à entrer dans le réseau d'une entreprise ainsi que le trafic informatique interne autorisé à entrer dans les zones de nature plus délicate du réseau de l'entreprise. Tous les systèmes ont besoin d'être protégés contre un accès non autorisé provenant d'Internet, que ce soit dans le cadre du commerce électronique, d'un accès à Internet par les employés ou d'un accès au courriel par les employés. Il arrive souvent qu'une transmission vers Internet ou en provenance d'Internet fournisse une voie d'accès non protégée à des systèmes clés. Les pare-feu constituent un mécanisme de protection essentiel à tout réseau informatique.

1.1 Établir des normes de configuration de pare-feu incluant :

- 1.1.1 un processus formel d'approbation et de vérification de toutes les connexions externes du réseau et de tous les changements apportés à la configuration du pare-feu;
- 1.1.2 un diagramme du réseau actuel et de toutes les connexions aux données des titulaires de carte, y compris tous les réseaux sans fil;
- 1.1.3 des exigences de pare-feu pour chaque connexion Internet et entre toute DMZ et l'intranet;
- 1.1.4 une description des groupes, des rôles et des responsabilités quant à la gestion logique des composantes du réseau;
- 1.1.5 une liste documentée des services / ports nécessaires à l'entreprise;
- 1.1.6 la justification et la documentation de tout protocole disponible, outre HTTP ainsi que SSL, SSH et VPN;
- 1.1.7 la justification et la documentation de tout protocole à risque autorisé (FTP, etc.), y compris la raison de l'utilisation du protocole et les caractéristiques de sécurité mises en œuvre;
- 1.1.8 la révision périodique de l'ensemble des règles de pare-feu / routeur;
- 1.1.9 les normes de configuration des routeurs.

1.2 Établir une configuration de pare-feu interdisant tout le trafic provenant de réseaux / hôtes « non sécurisés », **sauf** :

- 1.2.1 les protocoles Web - HTTP (port 80) et les protocoles de sécurisation (SSL) (en général, port 443);
- 1.2.2 les protocoles d'administration de système (par ex., SSH (Secure Shell) ou VPN (réseau virtuel privé));
- 1.2.3 autres protocoles requis par l'entreprise (par ex., pour ISO 8583).

1.3 Établir une configuration de pare-feu qui restreint les connexions entre les serveurs publiquement accessibles et toute composante du système où sont conservées des données des titulaires de carte, y compris toute connexion à partir d'un réseau sans fil. Cette configuration de pare-feu devrait :

- 1.3.1 restreindre le trafic entrant provenant d'Internet vers des adresses IP dans la DMZ (filtres d'entrée);
- 1.3.2 restreindre le trafic d'Internet entrant et sortant vers les ports 80 et 443;
- 1.3.3 ne pas autoriser des adresses internes à passer d'Internet à la DMZ (filtres de sortie);

- 1.3.4 comprendre un filtre dynamique à paquets (seules les connexions « établies » sont autorisées dans le réseau);

Établir et maintenir un réseau sécuritaire

- 1.3.5 placer la base de données dans une zone du réseau interne, séparée de la DMZ;
 - 1.3.6 restreindre le trafic sortant à ce qui est nécessaire à l'environnement des cartes de paiement;
 - 1.3.7 sécuriser et synchroniser les dossiers de configuration des routeurs (par ex., exécution des fichiers de configuration – utilisée pour les routeurs en temps normal, et exécution des fichiers de configuration de démarrage – utilisée lorsque les machines sont redémarrées, lesquelles devraient avoir la même configuration sécuritaire);
 - 1.3.8 interdire tout autre trafic entrant et sortant qui n'est pas spécifiquement autorisé;
 - 1.3.9 installer un pare-feu de périmètre entre tout réseau sans fil et l'environnement des cartes de paiement, et configurer ce pare-feu afin qu'il interdise ou contrôle (si ce trafic est nécessaire à des fins d'affaires) tout trafic provenant de l'environnement sans fil;
 - 1.3.10 installer un logiciel personnel de pare-feu sur tout ordinateur portable ou appartenant à un employé, qui a une connectivité directe à Internet (par ex., ordinateur portable utilisé par un employé) et qui sert à accéder au réseau de l'organisation.
- 1.4 Interdire l'accès public direct entre les réseaux externes et toute composante du système qui conserve de l'information sur les titulaires de carte (par ex., les bases de données).
- 1.4.1 Mettre en œuvre une DMZ pour filtrer et bloquer tout le trafic afin d'interdire les voies directes de trafic Internet entrant et sortant.
 - 1.4.2 Restreindre le trafic sortant provenant des applications de carte de paiement vers des adresses IP dans la DMZ.
- 1.5 Mettre en œuvre la mascarade IP afin d'éviter que des adresses internes soient traduites et révélées dans Internet. Utiliser une technologie qui met en œuvre la RFC 1918, comme PAT (Port Address Translation) ou NAT (Network Address Translation).

Exigence 2 : Ne pas utiliser les paramètres par défaut du fournisseur dans le cas des mots de passe et des autres paramètres de sécurité.

Les pirates (externes et internes) utilisent souvent les mots de passe et autres paramètres par défaut des fournisseurs pour compromettre des systèmes. Les mots de passe et ces paramètres sont bien connus des pirates et faciles à déterminer via l'information publique.

- 2.1 Toujours modifier les paramètres par défaut du fournisseur **avant** d'installer un système sur le réseau (par ex., mots de passe, noms de communauté SNMP et élimination des comptes inutiles).
 - 2.1.1 Dans le cas des environnements sans fil, modifier les paramètres par défaut du fournisseur, y compris, entre autres, les clés WEP, le SSID par défaut, les mots de passe et les noms de communauté SNMP, et désactiver la diffusion du SSID. Activer le protocole de cryptage et d'authentification WPA (Wi-Fi Protected Access), si le système supporte WPA.
- 2.2 Développer des normes de configuration pour toutes les composantes du système. S'assurer que ces normes tiennent compte des vulnérabilités connues en matière de sécurité et des pratiques exemplaires de l'industrie.

- 2.2.1 Mettre en œuvre une seule fonction primaire par serveur (*par ex., les serveurs Web, les serveurs de base de données et les serveurs DNS devraient être mis en œuvre sur des serveurs séparés*).

Établir et maintenir un réseau sécuritaire

- 2.2.2 Désactiver tous les services et les protocoles qui ne sont pas nécessaires et sécuritaires (*services et protocoles qui ne sont pas directement nécessaires à l'exécution d'une fonction précise*).
 - 2.2.3 Configurer les paramètres de sécurité du système afin de prévenir une utilisation abusive.
 - 2.2.4 Retirer toute fonctionnalité inutile, comme les messages, les pilotes, les caractéristiques, les sous-systèmes et les systèmes de fichier (*par ex., serveurs Web inutiles*).
- 2.3 Crypter tout accès administratif sans console. Utiliser des technologies comme SSH, VPN, ou SSL/TLS pour la gestion à partir du Web et tout autre accès administratif sans console.

Protéger les données des titulaires de carte

Exigence 3 : Protéger les données conservées.

Le cryptage est le meilleur mécanisme de protection, parce que, même si quelqu'un réussit à percer tous les autres mécanismes de protection et à avoir accès aux données cryptées, il ne pourra pas lire les données s'il n'en connaît pas le cryptage. Voilà qui illustre ce principe de défense en profondeur.

- 3.1** Conserver le moins d'information possible sur les titulaires de carte. Élaborer une politique en matière de conservation et de destruction des données. Limiter la quantité des données conservées et la durée de conservation à ce qui est nécessaire aux fins commerciales, juridiques et réglementaires, conformément à la politique en matière de conservation des données.
- 3.2** Ne pas conserver les données de nature délicate en matière d'authentification, à la suite d'une autorisation, (même si elles sont cryptées).
 - 3.2.1** Ne pas conserver le contenu intégral de toute trace d'une piste magnétique (au verso d'une carte, dans une puce, etc.).
 - 3.2.2** Ne pas conserver le code de vérification de la carte (numéro de trois chiffres ou de quatre chiffres, imprimé au recto ou au verso d'une carte de paiement (par ex., données CVV2 et CVC2)).
 - 3.2.3** Ne pas conserver la valeur de vérification du NIP (VVN).
- 3.3** Masquer les numéros de compte affichés (les six premiers chiffres et les quatre derniers chiffres constituent le nombre maximal de caractères qui peuvent être affichés).

Remarque : ceci ne s'applique pas aux employés et autres parties qui ont un besoin spécifique de voir le numéro complet de la carte de crédit.
- 3.4** Rendre illisibles les données de nature délicate des titulaires de carte, peu importe l'endroit où elles sont conservées (y compris les données des appareils portatifs, des supports de sauvegarde et des registres ainsi que les données provenant d'un réseau sans fil ou conservées dans un réseau sans fil) en utilisant l'une des approches suivantes :
 - le hachage à sens unique (index hachés), comme SHA-1;
 - la troncature;
 - les jetons d'index et les paquets de données, ces derniers étant conservés de façon sécuritaire;
 - un solide cryptage, comme Triple-DES à 128 bits ou AES à 256 bits, ainsi que les processus et procédures de gestion des clés connexes.

En ce qui a trait à l'information des comptes, on doit À TOUT LE MOINS rendre illisible le numéro de compte des cartes de paiement.
- 3.5** Protéger les clés de cryptage contre la divulgation et l'utilisation abusives.
 - 3.5.1** Restreindre l'accès aux clés de cryptage au plus petit nombre de gardiens possible.
 - 3.5.2** Conserver les clés de cryptage de façon sécuritaire dans le plus petit nombre d'endroits possible et sous le plus petit nombre de formes possible.
- 3.6** Bien documenter et mettre en œuvre tous les processus et procédures de gestion des clés de cryptage.
 - 3.6.1** Générer de solides clés de cryptage.
 - 3.6.2** Sécuriser la distribution des clés de cryptage.
 - 3.6.3** Sécuriser la conservation des clés de cryptage.
 - 3.6.4** Changer régulièrement les clés de cryptage.
 - 3.6.5** Détruire les anciennes clés de cryptage.

Protéger les données des titulaires de carte

- 3.6.6 Prévoir un double contrôle des clés de cryptage (de sorte qu'il faille deux ou trois personnes, ne connaissant chacune qu'une partie de la clé, pour reconstruire la totalité de la clé).
- 3.6.7 Prévenir une substitution non autorisée des clés de cryptage.
- 3.6.8 Remplacer les clés compromises ou soupçonnées de l'être.
- 3.6.9 Révoquer les anciennes clés ou les clés non valides (surtout les clés RSA).
- 3.6.10 Exiger que tous les gardiens des clés de cryptage signent un formulaire précisant qu'ils ont compris et acceptent leurs obligations en tant que gardien de clé.

Exigence 4 : Chiffrer la transmission des données des titulaires de carte et de l'information de nature délicate par le biais des réseaux publics.

L'information de nature délicate doit être chiffrée pendant sa transmission dans Internet, car il est facile et courant pour un pirate d'intercepter ou de détourner ces données pendant la transmission.

- 4.1 Utiliser de solides techniques de cryptographie et de chiffrement (au moins 128 bits), comme les protocoles SSL (Secure Sockets Layer), PPTP (Point-to-Point Tunneling Protocol) et IPSEC (Internet Protocol Security), pour protéger les données de nature délicate des titulaires de carte pendant leur transmission sur des réseaux publics.
 - 4.1.1 Dans le cas des réseaux sans fil transmettant des données des titulaires de carte, chiffrer les transmissions en utilisant la technologie WPA (Wi-Fi Protected Access), VPN ou SSL à 128 bits. Ne jamais se fier exclusivement à WEP pour protéger la confidentialité et l'accès à un LAN sans fil. Utiliser l'une des méthodologies ci-dessus, de concert avec WEP à 128 bits, et faire la rotation des clés WEP partagées, semestriellement et chaque fois qu'il y a un changement de personnel.
- 4.2 Ne jamais envoyer de renseignements sur les titulaires de carte par courriel non crypté.

Maintenir un programme de gestion de la vulnérabilité

Exigence 5 : Utiliser et mettre régulièrement à jour un logiciel d'anti-virus.

De nombreuses vulnérabilités et de nombreux virus malveillants entrent dans le réseau via le courriel des employés. On doit utiliser un anti-virus sur tous les systèmes de courriel et les postes de travail afin de protéger le réseau contre un logiciel malveillant.

- 5.1 Installer des anti-virus sur tous les systèmes couramment affectés par les virus (par ex., ordinateurs personnels et serveurs).
- 5.2 S'assurer que tous les anti-virus sont à jour, actifs et capables de produire des listes de contrôle.

Exigence 6 : Développer et maintenir des systèmes et des applications sécuritaires.

Des personnes sans scrupules utilisent les vulnérabilités de sécurité pour avoir un accès privilégié à des systèmes. Bon nombre de ces vulnérabilités se réparent au moyen des rustines de sécurité du fournisseur. Tous les systèmes devraient avoir les plus récentes rustines afin de se protéger contre une utilisation abusive par des employés, des pirates externes et des virus. Dans le cas des applications conçues à l'interne, de nombreuses vulnérabilités peuvent être évitées en utilisant des processus de développement de système normalisés et des techniques de codage sécuritaires.

- 6.1 S'assurer que toutes les composantes du système et tous les logiciels affichent les plus récentes rustines de sécurité du fournisseur.
 - 6.1.1 Installer les rustines de sécurité pertinentes au cours du mois suivant leur publication.
- 6.2 Établir un processus permettant de repérer les vulnérabilités de sécurité nouvellement découvertes (par ex., s'abonner à des services d'alerte offerts gratuitement dans Internet). Mettre vos normes à jour.
- 6.3 Élaborer des applications reposant sur les pratiques exemplaires de l'industrie et inclure la sécurité de l'information tout au long du cycle de l'élaboration des logiciels.
 - 6.3.1 Tester toutes les rustines de sécurité et tous les changements de configuration avant le déploiement.
 - 6.3.2 Séparer les environnements de développement ou de test et les environnements de production.
 - 6.3.3 Séparer les tâches entre les environnements de développement ou de test et les environnements de production.
 - 6.3.4 Les données de production (numéros de carte de crédit réels) ne doivent pas servir aux tests de développement.
 - 6.3.5 Retirer les données et les comptes ayant servis aux tests avant d'activer les systèmes de production.
 - 6.3.6 Retirer les comptes, les noms d'utilisateur et les mots de passe des applications maison avant d'activer ces applications ou de les transmettre aux clients.
 - 6.3.7 Examiner le code maison avant de transmettre l'application aux fins de production ou aux clients, afin d'identifier toute vulnérabilité potentielle du codage.
- 6.4 Suivre des procédures de contrôle pour tous les changements de configuration. Ces procédures devraient comprendre :
 - 6.4.1 la documentation de l'impact;
 - 6.4.2 l'autorisation signée des parties appropriées;

- 6.4.3 la vérification de la fonctionnalité opérationnelle;

Maintenir un programme de gestion de la vulnérabilité

- 6.4.4 les procédures de sauvegarde.
- 6.5 Élaborer un logiciel Web et des applications reposant sur des lignes directrices en matière de codage sécuritaire, comme celles de l'OWASP (Open Web Application Security Project). Vérifier le code d'application maison afin de repérer les vulnérabilités de codage. Voir www.owasp.org - *The Ten Most Critical Web Application Security Vulnerabilities*. Prévenir les vulnérabilités de codage courantes des processus de développement des logiciels, y compris :
- 6.5.1 les entrées non valides;
 - 6.5.2 un bris du contrôle d'accès (par ex., utilisation abusive d'un code d'utilisateur);
 - 6.5.3 un bris d'authentification ou de gestion d'une session (utilisation des données d'un compte et des cookies d'une session);
 - 6.5.4 les attaques XSS;
 - 6.5.5 les débordements de tampon;
 - 6.5.6 les attaques par injection (par ex., injection SQL);
 - 6.5.7 correction d'erreur inappropriée;
 - 6.5.8 conservation non sécuritaire;
 - 6.5.9 refus de service;
 - 6.5.10 gestion de configuration non sécuritaire.

Mettre en place de solides mesures de contrôle de l'accès

Exigence 7 : Restreindre l'accès aux données aux personnes qui ont besoin de les connaître.

Cette exigence permet d'assurer que les données de nature délicate ne sont accessibles que par les personnes autorisées.

- 7.1 Limiter l'accès aux ressources informatiques et à l'information sur les titulaires de carte aux seules personnes qui ont besoin d'y avoir accès dans le cadre de leur travail.
- 7.2 Établir un mécanisme applicable aux systèmes accessibles par de multiples utilisateurs, afin d'en restreindre l'accès aux personnes qui en ont besoin et de refuser tout autre accès qui n'a pas été spécifiquement autorisé.

Exigence 8 : Attribuer un code d'utilisateur unique à chaque personne ayant accès à l'ordinateur.

Cette exigence permet de s'assurer que les mesures prises relativement aux données et aux systèmes essentiels sont exécutées par des utilisateurs autorisés et connus, dont on peut assurer le suivi.

- 8.1 Identifier tous les usagers au moyen d'un code d'utilisateur unique avant de les autoriser à accéder aux composantes du système ou aux données des titulaires de carte.
- 8.2 Employer au moins une des méthodes ci-dessous, en plus d'un code d'utilisateur unique, pour authentifier tous les usagers :
 - mot de passe;
 - jetons (par ex., SecureID, certificats ou clé publique);
 - biométrie.
- 8.3 Mettre en œuvre une authentification à deux facteurs dans le cas de l'accès à distance au réseau par des employés, des administrateurs et des tierces parties. Utiliser des technologies, comme RADIUS ou TACACS avec des jetons, ou un VPN avec des certificats individuels.
- 8.4 Crypter tous les mots de passe avant la transmission et la conservation des données, sur toutes les composantes du système.
- 8.5 Assurer une authentification adéquate des utilisateurs et une gestion appropriée des mots de passe de tous les utilisateurs et administrateurs non consommateurs, sur toutes les composantes du système.
 - 8.5.1 Contrôler l'ajout, le retrait et la modification des codes d'utilisateur et des autres éléments d'identification.
 - 8.5.2 Vérifier l'identité de l'utilisateur avant de procéder à une modification du mot de passe.
 - 8.5.3 Établir un mot de passe initial unique pour chaque utilisateur et le modifier immédiatement après sa première utilisation.
 - 8.5.4 Annuler immédiatement l'accès des utilisateurs qui ne sont plus à l'emploi de l'entreprise.
 - 8.5.5 Retirer les comptes d'utilisateur inactifs au moins tous les 90 jours.
 - 8.5.6 N'activer les comptes utilisés par des fournisseurs à des fins d'entretien à distance que pendant la période nécessaire.
 - 8.5.7 Distribuer des procédures et des politiques en matière de mot de passe à tous les utilisateurs qui ont accès aux renseignements des titulaires de carte.
 - 8.5.8 Ne pas utiliser de comptes ou de mots de passe collectifs, partagés ou génériques.

Mettre en place de solides mesures de contrôle de l'accès

- 8.5.9 Modifier les mots de passe des utilisateurs au moins tous les 90 jours.
- 8.5.10 Exiger un mot de passe comportant au moins sept caractères.
- 8.5.11 Utiliser des mots de passe contenant à la fois des caractères numériques et alphabétiques.
- 8.5.12 Ne pas permettre à une personne de proposer un nouveau mot de passe similaire à l'un des quatre derniers mots de passe qu'elle a utilisés.
- 8.5.13 Limiter les tentatives d'accès répétées en bloquant le code d'utilisateur après six tentatives.
- 8.5.14 Fixer la durée du blocage à 30 minutes ou jusqu'à ce que l'administrateur active le code d'utilisateur.
- 8.5.15 Si une session est inactive pendant plus de 15 minutes, demander à l'utilisateur d'entrer de nouveau son mot de passe pour réactiver l'appareil.
- 8.5.16 Authentifier tous les accès à toute base de données contenant des renseignements sur les titulaires de carte. Ceci comprend l'accès par les applications, les administrateurs et tous les autres usagers.

Exigence 9 : Restreindre l'accès physique aux données des titulaires de carte.

Tout accès physique aux données ou aux systèmes contenant des données des titulaires de carte permet d'accéder à des appareils ou à des données et devrait être restreint de manière adéquate.

- 9.1 Utiliser des mesures de contrôle appropriées afin de limiter et de surveiller l'accès physique aux systèmes qui conservent, traitent ou transmettent des données sur les titulaires de carte.
 - 9.1.1 Utiliser des caméras pour surveiller les zones de nature délicate. Vérifier ces données en les comparant avec d'autres entrées. Les conserver pendant au moins trois mois, à moins que la loi l'interdise.
 - 9.1.2 Restreindre l'accès physique aux prises du réseau qui sont publiquement accessibles.
 - 9.1.3 Restreindre l'accès physique aux points d'accès sans fil, aux passerelles et aux appareils de poche.
- 9.2 Élaborer des procédures afin d'aider tout le personnel à faire aisément la distinction entre les employés et les visiteurs, surtout dans les zones où les renseignements sur les titulaires de carte sont accessibles.

Le terme « employé » fait référence aux employés à temps plein et à temps partiel, aux employés temporaires et aux consultants qui « résident » sur le site de l'organisation. Le terme « visiteur » fait référence aux fournisseurs, aux invités d'un employé, au personnel de service ou à quiconque a besoin d'entrer sur les lieux pour une courte période, n'excédant pas en général une journée.
- 9.3 Assurez-vous que tous les visiteurs :
 - 9.3.1 sont autorisés avant d'entrer dans les zones où les données de titulaires de carte sont traitées ou conservées;
 - 9.3.2 reçoivent un jeton (par ex., insigne ou dispositif d'accès) qui prévoit une date d'expiration et les identifie en tant que personnes ne faisant pas partie des employés;
 - 9.3.3 reçoivent l'instruction de remettre leur jeton avant de quitter les lieux ou à la date d'expiration.

Mettre en place de solides mesures de contrôle de l'accès

- 9.4** Utiliser un registre de visiteurs afin de conserver un suivi de leurs activités. Conserver ce registre pendant au moins trois mois, à moins que la loi l'interdise.
- 9.5** Conserver les sauvegardes dans un endroit sécuritaire hors site. Il peut s'agir d'une installation d'entreposage commerciale ou appartenant à un tiers.
- 9.6** Assurer la sécurité physique de tous les supports papier et électroniques (par ex., ordinateurs, supports électroniques, matériel de réseautage et de communication, lignes de télécommunication, reçus papier, rapports papier et télécopies) qui contiennent des renseignements sur les titulaires de carte.
- 9.7** Maintenir un contrôle strict sur la distribution interne ou externe de tous les types de supports contenant des renseignements sur les titulaires de carte.
 - 9.7.1** Étiqueter les supports de manière à ce qu'ils soient identifiés comme étant confidentiels.
 - 9.7.2** Envoyer les supports par messagerie sécuritaire ou au moyen d'un mécanisme de livraison qui peut être retracé avec précision.
- 9.8** S'assurer que la gestion couvre tous les supports qui sont déménagés d'une zone sécuritaire (surtout lorsqu'il s'agit d'un support distribué à des particuliers).
- 9.9** Maintenir un contrôle strict sur la conservation et l'accessibilité des supports qui contiennent des renseignements sur les titulaires de carte.
 - 9.9.1** Répertorier adéquatement tous les supports et s'assurer qu'ils sont conservés de façon sécuritaire.
- 9.10** Détruire les supports contenant des renseignements sur les titulaires de carte, lorsqu'ils ne sont plus requis à des fins commerciales ou pour des raisons légales.
 - 9.10.1** Déchiqueter avec coupe en travers, incinérer ou réduire en pulpe les documents papier.
 - 9.10.2** Éliminer, démagnétiser, déchiqueter ou détruire par un autre moyen les supports électroniques, de manière à ce que les données des titulaires de carte ne puissent être reconstruites.

Surveiller et tester régulièrement les réseaux

Exigence 10 : Assurer un suivi et une surveillance de tout accès aux ressources du réseau et aux données des titulaires de carte.

Les dispositifs d'enregistrement et la capacité de retracer les activités des utilisateurs sont des éléments essentiels. La présence de registres dans tous les environnements permet d'effectuer un suivi et une analyse approfondis lorsque survient un problème. Il est très difficile de déterminer la cause d'une compromission lorsqu'il n'existe aucun registre des activités du système.

- 10.1** Établir un processus pour relier tous les accès d'un utilisateur aux composantes du système (surtout les accès assortis d'un privilège administratif ou racine).
- 10.2** Mettre en œuvre des listes de contrôle automatisées afin de reconstituer les événements suivants, pour toutes les composantes du système.
 - 10.2.1** Tous les accès d'un utilisateur ou données d'un titulaire de carte
 - 10.2.2** Toutes les mesures prises par un utilisateur ayant un privilège administratif ou racine
 - 10.2.3** L'accès à toutes les listes de contrôle
 - 10.2.4** Les tentatives non valides d'accès logique
 - 10.2.5** L'utilisation d'un mécanisme d'identification et d'authentification
 - 10.2.6** L'initialisation des registres de vérification
 - 10.2.7** La création et l'annulation d'éléments au niveau du système
- 10.3** Enregistrer au moins les entrées de liste de contrôle suivantes pour chaque événement, pour toutes les composantes du système.
 - 10.3.1** Code d'utilisateur
 - 10.3.2** Type d'événement
 - 10.3.3** Date et heure
 - 10.3.4** Réussite ou échec
 - 10.3.5** Origine de l'événement
 - 10.3.6** Identité ou nom des données, de la composante du système ou de la ressource affectées
- 10.4** Synchroniser toutes les horloges et les heures du système qui sont essentiels.
- 10.5** Sécuriser les listes de contrôle de manière à ce qu'elles ne puissent être modifiées, y compris ce qui suit.
 - 10.5.1** Limiter la consultation des listes de contrôle aux personnes qui en ont besoin dans le cadre de leur travail.
 - 10.5.2** Protéger les dossiers des listes de contrôle contre les modifications non autorisées.
 - 10.5.3** Effectuer rapidement une sauvegarde des dossiers des listes de contrôle dans un serveur de registre ou un support centralisé, difficile à modifier.
 - 10.5.4** Copier les registres des réseaux sans fil sur un serveur de registre du LAN interne.
 - 10.5.5** Utiliser un logiciel de suivi ou de détection des changements de l'intégrité (comme *Tripwire*) dans le cas des registres afin d'assurer que les données des registres existants ne peuvent pas être modifiées sans générer des alertes (quoique l'ajout de nouvelles données ne devrait pas susciter d'alerte).
- 10.6** Passer en revue les registres de toutes les composantes du système au moins une fois par jour. La révision des registres devrait inclure les serveurs qui exécutent des fonctions de sécurité comme IDS et les serveurs d'authentification (AAA) (par ex., RADIUS).

Surveiller et tester régulièrement les réseaux

- 10.7** Conserver les registres des listes de contrôle pendant une période correspondant à leur utilisation et à la réglementation.
- Les antécédents de vérification couvrent en général une période d'au moins un an, dont un minimum de trois mois sont disponibles en ligne.*

Exigence 11 : Tester régulièrement les systèmes et les processus de sécurité.

Les pirates et les chercheurs découvrent sans cesse des vulnérabilités qui sont introduites par de nouveaux logiciels. Les systèmes, les processus et les logiciels maison devraient être testés fréquemment afin d'en assurer la sécurité à long terme et lors de changements.

- 11.1** Tester régulièrement les mesures de contrôle de la sécurité, les limites, les connexions au réseau et les restrictions afin d'assurer qu'elles peuvent identifier ou contrer adéquatement toutes les tentatives d'accès non autorisées. Dans le cas de la technologie sans fil, utiliser régulièrement un analyseur sans fil pour identifier tous les appareils sans fil en usage.
- 11.2** Procéder à des balayages de la vulnérabilité des réseaux interne et externe au moins chaque trimestre et après chaque changement important apporté au réseau (par ex., nouvelles composantes informatiques, changement de la topologie du réseau, modification des règles de pare-feu, mise à niveau d'un produit).
- Soulignons que les balayages de vulnérabilité externe doivent être exécutés par un fournisseur qualifié par l'industrie des cartes de paiement.*
- 11.3** Exécuter des tests de pénétration sur l'infrastructure du réseau et les applications au moins une fois l'an et après toute amélioration ou modification importante à l'infrastructure ou aux applications (par ex., mise à niveau du système d'exploitation, ajout d'un sous-réseau à l'environnement, ajout d'un serveur Web à l'environnement).
- 11.4** Utiliser des systèmes de détection des intrusions au réseau, des systèmes de détection des intrusions à partir d'un hôte et(ou) des systèmes de prévention des intrusions pour surveiller tout le trafic du réseau et alerter le personnel en cas de doute quant à la compromission du système. Conserver à jour tous les mécanismes de prévention et de détection des intrusions.
- 11.5** Prévoir un mécanisme de surveillance de l'intégrité des dossiers afin de prévenir le personnel de toute modification non autorisée d'un système essentiel ou des fichiers de contenu, et effectuer des comparaisons des fichiers essentiels au moins une fois par jour (ou plus fréquemment si le processus peut être automatisé).
- Les fichiers essentiels ne sont pas nécessairement ceux qui renferment les données des titulaires de carte. Aux fins de surveillance de l'intégrité des fichiers, les fichiers essentiels sont en général ceux qui ne changent pas régulièrement, mais dont la modification peut indiquer une compromission ou un risque de compromission du système. Les produits de surveillance de l'intégrité des fichiers sont en général configurés à l'avance et comportent des fichiers essentiels pour le système d'exploitation connexe. Les autres fichiers essentiels, comme ceux des applications maison, doivent être évalués et définis par le marchand ou le fournisseur de services.*

Maintenir une politique de sécurité de l'information

Exigence 12 : Maintenir une politique en matière de sécurité de l'information à l'intention des employés et des contractuels.

Une solide politique en matière de sécurité permet de donner le ton à l'ensemble de l'entreprise et de laisser savoir aux employés ce que l'on attend d'eux. Tous les employés devraient être au courant de la nature délicate des données et de leurs responsabilités pour en assurer la protection.

- 12.1** Établir, publier, tenir à jour et diffuser une politique en matière de sécurité :
 - 12.1.1** tenant compte de toutes les exigences de la présente norme;
 - 12.1.2** incluant un processus annuel qui identifie les menaces et les vulnérabilités et qui donne lieu à une évaluation officielle du risque;
 - 12.1.3** incluant un examen au moins une fois l'an et une mise à jour chaque fois que des changements sont apportés à l'environnement.
- 12.2** Élaborer des procédures de sécurité opérationnelle quotidiennes qui sont en conformité avec les exigences de la présente norme (par ex., procédures de tenue des comptes d'utilisateur, procédures d'examen des registres).
- 12.3** Élaborer des politiques d'utilisation relativement aux technologies essentielles reliées aux employés, comme les modems et les appareils sans fil, afin de définir l'usage adéquat de ces technologies pour tous les employés et les contractuels. S'assurer que ces politiques d'utilisation comportent les exigences suivantes :
 - 12.3.1** approbation explicite de la gestion;
 - 12.3.2** authentification pour l'utilisation de la technologie;
 - 12.3.3** liste de tous ces appareils et du personnel qui y a accès;
 - 12.3.4** étiquetage des appareils, y compris le nom du propriétaire, ses coordonnées et les fins pour lesquelles ils sont utilisés;
 - 12.3.5** utilisations acceptables de la technologie;
 - 12.3.6** endroits acceptables du réseau pour ces technologies;
 - 12.3.7** liste des produits approuvés par l'entreprise;
 - 12.3.8** débranchement automatique des sessions de modem après une certaine période d'inactivité;
 - 12.3.9** activation des modems pour les fournisseurs, uniquement lorsqu'ils en ont besoin, suivie d'une désactivation immédiate après l'utilisation;
 - 12.3.10** dans le cas d'un accès à distance aux données des titulaires de carte par modem, désactivation de la conservation des données des titulaires de carte sur les disques durs locaux, les disquettes ou un autre support externe; désactivation des fonctions « couper-coller » et des fonctions d'impression pendant l'accès à distance.
- 12.4** S'assurer que la politique et les procédures en matière de sécurité définissent clairement les responsabilités de tous les employés et contractuels en ce qui a trait à la sécurité de l'information.
- 12.5** Attribuer à une personne ou à une équipe les responsabilités suivantes en matière de gestion de la sécurité de l'information.
 - 12.5.1** Établir, documenter et diffuser les politiques et les procédures en matière de sécurité.
 - 12.5.2** Surveiller et analyser les alertes et l'information en matière de sécurité, et transmettre ces renseignements au personnel approprié.

Maintenir une politique de sécurité de l'information

- 12.5.3** Établir, documenter et distribuer des procédures d'intervention et de recours à la hiérarchie en matière de sécurité afin d'assurer une gestion efficace et rapide de toutes les situations.
 - 12.5.4** Administrer les comptes d'utilisateur, y compris les ajouts, les retraits et les modifications.
 - 12.5.5** Surveiller et contrôler tous les accès aux données.
- 12.6** Informer tous les employés de l'importance de la sécurité des renseignements des titulaires de carte.
 - 12.6.1** Informer les employés (par ex., au moyen d'affiches, de lettres, de notes de service, de réunions et de promotions).
 - 12.6.2** Demander aux employés de confirmer par écrit qu'ils ont lu et compris la politique et les procédures de l'entreprise en matière de sécurité.
- 12.7** Sélectionner les employés potentiels afin de réduire au minimum le risque d'attaques provenant de sources internes.

Dans les cas des employés qui ont uniquement accès à un seul numéro de carte à la fois pour faciliter une transaction, comme dans le cas des caissiers des magasins, cette exigence n'est qu'une recommandation.
- 12.8** Exiger par contrat que toutes les tierces parties ayant accès aux données des titulaires de carte adhèrent aux exigences de sécurité de l'industrie des cartes de paiement. À tout le moins, l'entente devrait comprendre ce qui suit :
 - 12.8.1** une attestation selon laquelle la tierce partie est responsable d'assurer la sécurité des données des titulaires de carte en sa possession;
 - 12.8.2** la propriété par marque de carte de paiement, acquéreur et marchand des données des titulaires de carte et une attestation selon laquelle ces données ne peuvent être utilisées que pour aider ces parties à effectuer une transaction, à soutenir un programme de fidélité, à fournir des services de contrôle de la fraude ou à d'autres fins spécifiquement prévues par la loi;
 - 12.8.3** la continuité des affaires en cas d'interruption majeure, de désastre ou de panne importante;
 - 12.8.4** des dispositions de vérification qui assurent que le représentant de l'industrie des cartes de paiement, ou une tierce partie approuvée par l'industrie des cartes de paiement, obtiendra la pleine collaboration et l'accès nécessaires pour mener à bien un examen approfondi de la sécurité à la suite d'une intrusion; cet examen validera la conformité à la *Norme de sécurité des données de l'industrie des cartes de paiement* relativement à la protection des données des cartes;
 - 12.8.5** une clause d'expiration qui assure que la tierce partie continuera de traiter les données des titulaires de carte de manière confidentielle.
- 12.9** Mettre en œuvre un plan d'intervention en cas d'incident. Être prêt à réagir immédiatement à un bris de système.
 - 12.9.1** Créer un plan d'intervention à utiliser en cas de compromission du système. S'assurer que le plan prévoit, à tout le moins, des procédures d'intervention spécifiques, des procédures de récupération et de continuité, des processus de sauvegarde des données, les rôles et les responsabilités ainsi que des stratégies de communication (par ex., informer les acquéreurs et les associations de cartes de crédit).
 - 12.9.2** Tester le plan au moins une fois l'an.

- 12.9.3** Désigner des employés qui devront être disponibles en tout temps pour réagir aux alertes.

Maintenir une politique de sécurité de l'information

- 12.9.4** Fournir une formation appropriée au personnel en ce qui a trait aux responsabilités d'intervention en cas de compromission.
- 12.9.5** Prévoir des alertes permettant de déceler des intrusions, des mesures de prévention contre les intrusions et des systèmes de surveillance de l'intégrité des fichiers.
- 12.9.6** Prévoir un processus pour modifier et adapter le plan d'intervention en fonction des leçons apprises et pour intégrer les développements de l'industrie.