



**Payment Card Industry (PCI)
Data Security Standard**

Navigation dans les normes PCI DSS

Comprendre l'objectif des exigences

Version 1.2

Octobre 2008

Modifications apportées au document

<i>Date</i>	<i>Version</i>	<i>Description</i>
1 ^{er} octobre 2008	1.2	Aligner le contenu avec la nouvelle procédure PCI DSS v1.2 et implémenter les changements mineurs notés depuis la v1.1 d'origine.

Table des matières

Modifications apportées au document	i
Avant-propos	iii
Éléments de données de titulaire de carte et de données d'authentification sensibles	1
<i>Emplacement des données de titulaire de carte et des données d'authentification sensibles</i>	2
<i>Données de Piste 1 et de Piste 2</i>	3
Directives relatives aux normes PCI DSS	4
Directives relatives aux exigences 1 et 2 : Création et gestion d'un réseau sécurisé	5
<i>Exigence 1 : Installer et gérer une configuration de pare-feu pour protéger les données de titulaire de carte</i>	5
<i>Exigence 2 : Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur</i>	10
Directives relatives aux exigences 3 et 4 : Protection des données de titulaire de carte de crédit	13
<i>Exigence 3 : Protéger les données de titulaire de carte stockées</i>	13
<i>Exigence 4 : Crypter la transmission des données de titulaire de carte sur les réseaux publics ouverts</i>	19
Directives relatives aux exigences 5 et 6 : Gestion d'un programme de gestion des vulnérabilités	21
<i>Exigence 5 : Utiliser des logiciels antivirus et les mettre à jour régulièrement</i>	21
<i>Exigence 6 : Développer et gérer des systèmes et des applications sécurisés</i>	23
Directives relatives aux exigences 7, 8 et 9 : Mise en œuvre de mesures de contrôle d'accès strictes	30
<i>Exigence 7 : Restreindre l'accès aux données de titulaire de carte aux seuls individus qui doivent les connaître</i>	30
<i>Exigence 8 : Affecter un ID unique à chaque utilisateur d'ordinateur</i>	32
<i>Exigence 9 : Restreindre l'accès physique aux données de titulaire de carte</i>	36
Directives relatives aux exigences 10 et 11 : Surveillance et test réguliers des réseaux	41
<i>Exigence 10 : Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données de titulaire de carte</i>	41
<i>Exigence 11 : Tester régulièrement les processus et les systèmes de sécurité</i>	45
Directives relatives à l'exigence 12 : Gestion d'une politique de sécurité des informations	48
<i>Exigence 12 : Gérer une politique qui assure la sécurité des informations des employés et des sous-traitants</i>	48
Directives relatives à l'exigence A.1 : Autres exigences des normes PCI DSS s'appliquant aux fournisseurs d'hébergement partagé	54
Annexe A : Normes PCI DSS : documents connexes	56

Avant-propos

Le présent document décrit les douze exigences des normes de sécurité des données de la Payment Card Industry (PCI DSS) et explique l'objectif de chacune d'elles. Il vise à aider les commerçants, les prestataires de services et les établissements financiers qui souhaitent se faire une idée plus claire des normes de sécurité des données de la Payment Card Industry et mieux cerner la signification et l'intention de chaque exigence de sécurisation des composants du système (serveurs, réseau, applications, etc.) qui prennent en charge les environnements des données de titulaire de carte.

REMARQUE : Le document *Navigation dans les normes PCI DSS : comprendre l'objectif des exigences* est fourni à titre d'information seulement. Lorsque vous réalisez une évaluation sur site PCI DSS ou complétez un questionnaire d'auto-évaluation (SAQ), vous devez vous référer aux documents intitulés *Normes de sécurité des données de la Payment Card Industry (PCI DSS) - Conditions et procédures d'évaluation de sécurité* et aux *Questionnaires d'auto-évaluation sur les normes PCI DSS version 1.2*.

Les exigences des normes PCI DSS s'appliquent à tous les composants du système qui sont installés dans l'environnement des données de titulaire de carte ou qui sont connectés à cet environnement. L'environnement des données de titulaire de carte correspond à la partie du réseau qui contient les données de titulaire de carte ou les données d'authentification sensibles, notamment les applications, les serveurs et les composants réseau.

- Les composants réseau peuvent comprendre notamment les pare-feu, les commutateurs, les routeurs, les points d'accès sans fil, les équipements réseau et d'autres appareils de sécurité.
- Les types de serveurs peuvent comprendre notamment les serveurs Web, de base de données, d'authentification, de messagerie, proxy, NTP (Network Time Protocol) et DNS (Domain Name Server).
- Les applications peuvent comprendre notamment toutes les applications achetées et personnalisées, y compris les applications internes et externes (Internet).

Une bonne segmentation réseau, qui isole les systèmes qui stockent, traitent ou transmettent les données de titulaire de carte des autres, peut contribuer à réduire la portée de l'environnement des données de titulaire de carte. Un évaluateur de sécurité qualifié (QSA) peut aider à déterminer la portée dans l'environnement des données de titulaire de carte d'une entité ainsi qu'à réduire la portée d'une évaluation PCI DSS en mettant en œuvre la segmentation réseau appropriée. Si vous avez des questions concernant la conformité d'une mise en œuvre particulière avec les normes ou avec une exigence spécifique, PCI SSC recommande aux entreprises de consulter un évaluateur de sécurité qualifié (QSA) pour valider leur mise en œuvre de la technologie ou des processus, et leur respect des normes PCI DSS. Grâce à son expérience des environnements réseau complexes, l'évaluateur est en mesure de recommander les meilleures pratiques et d'orienter le commerçant ou le prestataire de services en vue de se mettre en conformité avec les normes. La liste des évaluateurs de sécurité qualifiés PCI SSC est disponible à l'adresse suivante : https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf.

Éléments de données de titulaire de carte et de données d'authentification sensibles

Le tableau suivant présente un certain nombre d'éléments courants des données de titulaire de carte et des données d'authentification sensibles, indique si le **stockage** de ces données est autorisé ou interdit, et précise si chaque élément de données doit être **protégé**. Ce tableau n'est pas exhaustif, mais il est présenté de manière à illustrer les divers types d'exigences qui s'appliquent à chaque élément de données.

Les données de titulaire de carte sont définies comme le PAN (Primary Account Number ou numéro de compte principal) et les autres données obtenues dans le cadre d'une transaction de paiement, notamment les éléments de données suivants (voir les détails ci-dessous dans le tableau) :

- PAN
- Nom du titulaire de carte
- Date d'expiration
- Code de service
- Données d'authentification sensibles : (1) intégralité des données de bande magnétique, (2) CAV2/CVC2/CVV2/CID et (3) blocs/codes PIN)

Le PAN (Primary Account Number ou numéro de compte principal) est le facteur de définition des conditions d'application des exigences PCI DSS et de la norme PA-DSS. Si le PAN n'est pas stocké, traité ou transmis, les normes PCI DSS et PA-DSS ne s'appliquent pas.

	Élément de données	Stockage autorisé	Protection requise	Exig. PCI DSS 3, 4
Données de titulaire de carte de crédit	PAN	Oui	Oui	Oui
	Nom du titulaire de la carte de crédit ¹	Oui	Oui ¹	Non
	Code service ¹	Oui	Oui ¹	Non
	Date d'expiration ¹	Oui	Oui ¹	Non
Données d'authentification sensibles ²	Données de bande magnétique complètes ³	Non	s.o.	s.o.
	CAV2/CVC2/CVV2/CID	Non	s.o.	s.o.
	Bloc/Code PIN	Non	s.o.	s.o.

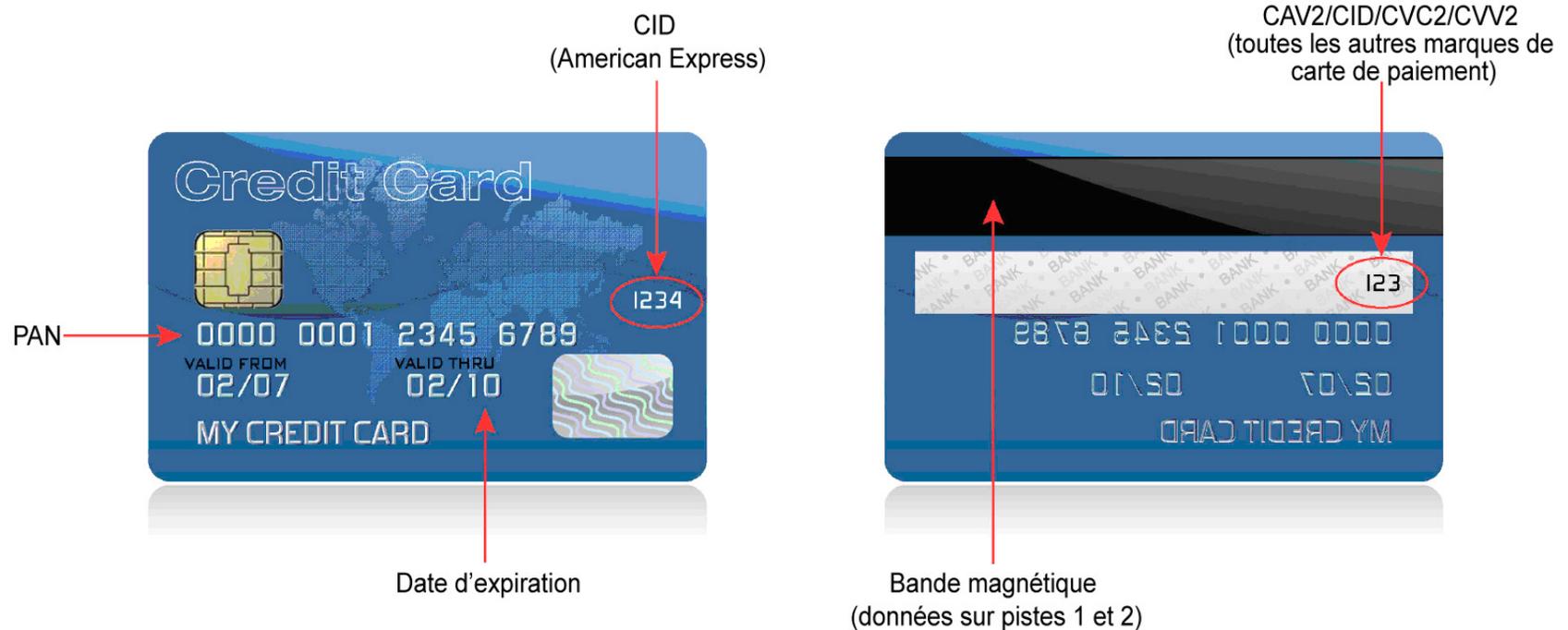
¹ Ces éléments de données doivent être protégés s'ils sont stockés conjointement avec le PAN. Cette protection doit être conforme aux exigences PCI DSS en liaison avec la protection générale de l'environnement des titulaires de carte. En outre, d'autres lois (par exemple, relatives à la protection des données personnelles des consommateurs, à la confidentialité, à l'usurpation d'identité ou à la sécurité des données) peuvent imposer une protection spécifique de ces données, ou une divulgation adéquate des pratiques de la société dès lors que des données à caractère personnel sont collectées dans le cadre de l'activité. Toutefois, les normes PCI DSS ne s'appliquent pas si des PAN ne sont pas stockés, traités ou transmis.

² Une fois le processus d'autorisation terminé, les données d'authentification sensibles ne peuvent plus être stockées (même si elles sont cryptées).

³ Données de piste complètes extraites de la bande magnétique, de l'image de la bande magnétique sur la puce ou d'un autre support.

Emplacement des données de titulaire de carte et des données d'authentification sensibles

Les données d'authentification sensibles consistent en les données de bande (ou piste) magnétique⁴, le code ou la valeur de validation de carte⁵ et le code PIN⁶. **Le stockage des données d'authentification sensibles est interdit !** Ces données sont précieuses pour les individus malveillants car elles leur permettent de créer de fausses cartes de paiement et des transactions frauduleuses. Voir la définition intégrale des « données d'authentification sensibles » dans le *Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS*. Les illustrations des faces recto et verso d'une carte bancaire ci-dessous indiquent l'emplacement des données de titulaire de carte et des données d'authentification sensibles.



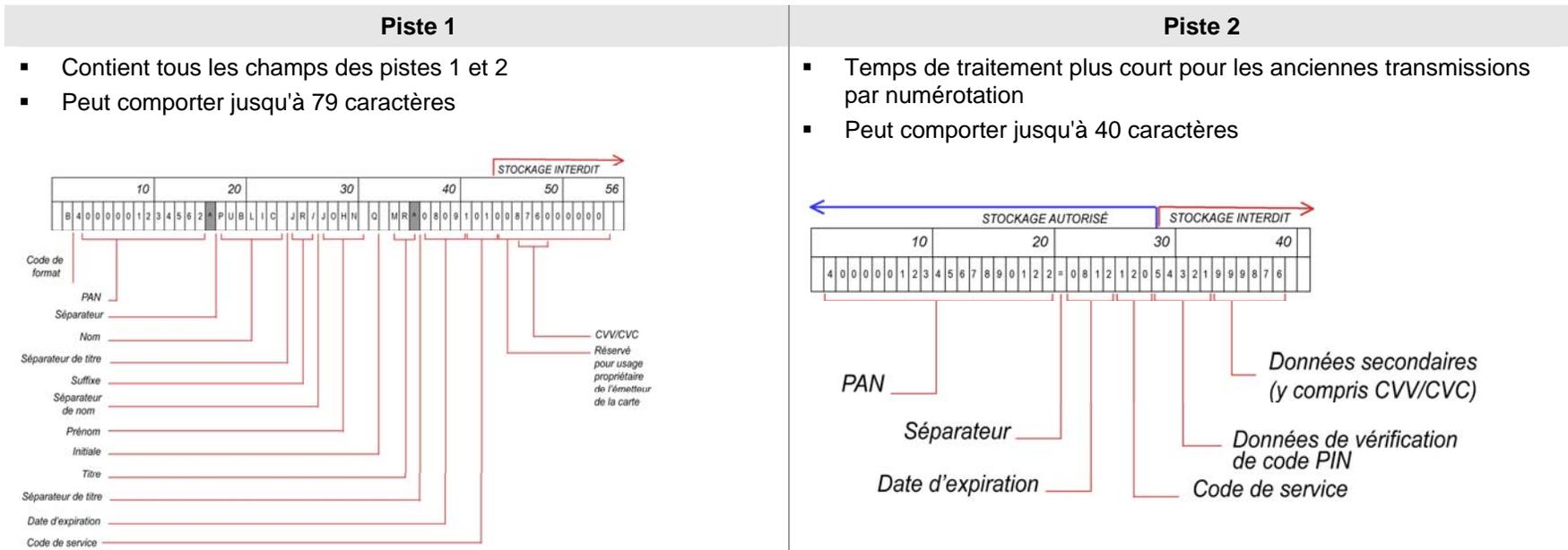
⁴ Données encodées sur la bande magnétique utilisée pour une autorisation lors d'une transaction carte présente. Ces données peuvent également se trouver dans l'image de la bande magnétique sur la puce ou sur un autre support de la carte. Les entités ne doivent pas conserver l'ensemble des données sur bande magnétique après l'autorisation des transactions. Les seuls éléments des données de piste pouvant être conservés sont le PAN, le nom du titulaire de carte, la date d'expiration et le code de service.

⁵ La valeur à trois ou quatre chiffres imprimée à droite de l'espace dédié à la signature ou sur la face d'une carte de paiement, utilisée pour vérifier les transactions carte absente.

⁶ Les données PIN (Personal Identification Number, numéro d'identification personnel) saisies par le titulaire de la carte lors d'une transaction carte présente et/ou le bloc PIN crypté présent dans le message de la transaction.

Données de Piste 1 et de Piste 2

Si les données de piste (Piste 1 ou Piste 2, bande magnétique, image de la bande magnétique sur une puce, ou autre support) complètes étaient stockées, les individus malveillants qui parviennent à se les procurer pourraient reproduire et vendre des cartes de paiement à travers le monde. Le stockage des données de piste complètes contrevient également aux réglementations régissant les activités des marques de cartes de paiement et est sanctionné par des amendes et des pénalités. L'illustration ci-dessous fournit des informations sur les données de Piste 1 et Piste 2, en décrivant les différences qui existent entre elles ainsi que la manière dont elles sont stockées sur la bande magnétique.



Directives relatives aux normes PCI DSS

Création et gestion d'un réseau sécurisé

- Exigence 1 : Installer et gérer une configuration de pare-feu pour protéger les données de titulaire de carte
Exigence 2 : Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur

Protection des données de titulaire de carte de crédit

- Exigence 3 : Protéger les données de titulaire de carte stockées
Exigence 4 : Crypter la transmission des données de titulaire de carte sur les réseaux publics ouverts

Gestion d'un programme de gestion des vulnérabilités

- Exigence 5 : Utiliser des logiciels antivirus et les mettre à jour régulièrement
Exigence 6 : Développer et gérer des systèmes et des applications sécurisés

Mise en œuvre de mesures de contrôle d'accès strictes

- Exigence 7 : Restreindre l'accès aux données de titulaire de carte aux seuls individus qui doivent les connaître
Exigence 8 : Affecter un ID unique à chaque utilisateur d'ordinateur
Exigence 9 : Restreindre l'accès physique aux données de titulaire de carte

Surveillance et test réguliers des réseaux

- Exigence 10 : Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données de titulaire de carte
Exigence 11 : Tester régulièrement les processus et les systèmes de sécurité

Gestion d'une politique de sécurité des informations

- Exigence 12 : Gérer une politique de sécurité des informations

Directives relatives aux exigences 1 et 2 : Création et gestion d'un réseau sécurisé

Exigence 1 : Installer et gérer une configuration de pare-feu pour protéger les données de titulaire de carte

Les pare-feu sont des dispositifs informatiques qui contrôlent le trafic autorisé entre le réseau d'une entreprise (interne) et les réseaux non approuvés (externes), ainsi que le trafic entrant et sortant dans des zones plus sensibles du réseau approuvé interne d'une société. L'environnement des données de titulaire de carte est un exemple de zone plus sensible au sein du réseau approuvé d'une société.

Un pare-feu examine l'ensemble du trafic réseau et bloque les transmissions qui ne satisfont pas aux critères de sécurité définis.

Tous les systèmes doivent être protégés contre les accès non autorisés depuis un réseau non approuvé, que ce soit en entrée via Internet (par exemple e-commerce, accès des employés à Internet à partir de leurs navigateurs, accès des employés à la messagerie électronique, connexions dédiées telles que les connexions interentreprises) ou bien via les réseaux sans fil ou d'autres sources. Les chemins d'accès de/vers des réseaux non approuvés, en apparence insignifiants, peuvent souvent constituer des chemins d'accès non protégés à des systèmes critiques. Les pare-feu sont des mécanismes de protection essentiels sur tout réseau informatique.

Exigence	Directive
<p>1.1 Définir des normes de configuration des pare-feu et des routeurs incluant les éléments suivants :</p>	<p>Les pare-feu et les routeurs sont les composants essentiels de l'architecture contrôlant les entrées et les sorties sur le réseau. Il s'agit de dispositifs logiciels ou matériels qui bloquent les accès indésirables et gèrent les accès autorisés de/vers le réseau. Sans la mise en place de politiques et de procédures indiquant au personnel comment configurer les pare-feu et les routeurs, une société pourrait facilement perdre sa première ligne de défense en matière de protection des données. Ces politiques et procédures l'aideront à maintenir la robustesse de sa première ligne de défense.</p>
<p>1.1.1 Processus formel d'approbation et de test de toutes les connexions réseau externes et des modifications apportées aux configurations des pare-feu et des routeurs</p>	<p>Une politique et un processus d'approbation et de test de toutes les connexions et des modifications apportées aux configurations des pare-feu et des routeurs contribueront à éviter les problèmes de sécurité dus aux erreurs de configuration du réseau, d'un routeur ou d'un pare-feu.</p>
<p>1.1.2 Schéma de réseau actuel indiquant toutes les connexions aux données de titulaire de carte, notamment tous les réseaux sans fil</p>	<p>Les schémas de réseau permettent à l'entreprise d'identifier l'emplacement de tous ses périphériques réseau. En outre, ces schémas peuvent servir au mappage des flux des données de titulaire de carte à travers le réseau et entre des dispositifs individuels en vue de bien comprendre la portée de l'environnement des données de titulaire de carte. Sans ces schémas de réseaux et des flux de données actualisés, des dispositifs comprenant des données de titulaire de carte peuvent être négligés et peuvent échapper par mégarde aux contrôles de sécurité mis en place dans le cadre des normes PCI DSS. Ils sont alors exposés à des risques.</p>

Exigence	Directive
<p>1.1.3 Exigence d'un pare-feu au niveau de chaque connexion Internet et entre toute zone démilitarisée (DMZ) et la zone de réseau interne</p>	<p>L'utilisation d'un pare-feu sur chaque connexion entrante (et sortante) du réseau permet à l'entreprise de surveiller et de contrôler les accès en entrée et en sortie, et de réduire les risques qu'un individu malveillant parvienne à accéder au réseau interne.</p>
<p>1.1.4 Description des groupes, des rôles et des responsabilités pour la gestion logique des composants réseau</p>	<p>Cette description des rôles et des responsabilités garantit qu'une personne est clairement responsable de la sécurité de tous les composants et a parfaitement conscience de cette responsabilité, et qu'aucun appareil n'échappe à cette gestion.</p>
<p>1.1.5 Documentation et justification professionnelle de l'utilisation de tous les services, protocoles et ports autorisés, y compris la documentation des fonctions de sécurité mises en œuvre pour les protocoles considérés comme étant non sécurisés</p>	<p>Les risques sont souvent dus à la présence de services et de ports non utilisés ou non sécurisés, dont les vulnérabilités sont souvent connues. De nombreuses entreprises s'exposent à ces types de risques car elles ne mettent pas en place les correctifs de sécurité nécessaires pour les services, les protocoles et les ports qu'elles n'utilisent pas (même si les vulnérabilités persistent). Chaque entreprise doit clairement déterminer les services, les protocoles et les ports nécessaires à la conduite de ses activités, les consigner dans ses archives et veiller à ce que tous les autres services, protocoles et ports soient désactivés ou supprimés. En outre, les entreprises doivent envisager de bloquer l'ensemble du trafic et de ne rouvrir les ports concernés qu'en cas de besoin avéré.</p> <p>Par ailleurs, de nombreux services, protocoles ou ports qu'une entreprise peut nécessiter (ou qu'elle a activés par défaut) sont fréquemment utilisés par les individus malveillants pour s'introduire sur un réseau. Si ces services, protocoles ou ports non sécurisés sont nécessaires aux activités de l'entreprise, les risques qu'ils impliquent doivent être bien compris et admis par l'entreprise. Leur usage doit être justifié et les fonctions de sécurité permettant leur utilisation de manière sécurisée doivent être documentées et mises en place. Si ces services, protocoles ou ports non sécurisés ne sont pas nécessaires aux activités de la société, ils doivent être désactivés ou supprimés.</p>
<p>1.1.6 Nécessité d'examiner les règles des pare-feu et des routeurs au moins tous les six mois</p>	<p>Cet examen permet à l'entreprise, au moins tous les six mois, d'éliminer les règles superflues, obsolètes ou incorrectes, et de veiller à ce que toutes les règles n'admettent que les services et les ports autorisés dont l'usage est justifié.</p> <p>Il est recommandé d'effectuer ces examens plus fréquemment, par exemple une fois par mois, afin de veiller à ce que les règles soient actualisées et satisfassent aux besoins de l'entreprise, sans ouvrir de failles en termes de sécurité et de courir des risques superflus.</p>

Exigence	Directive
<p>1.2 Créer une configuration de pare-feu qui limite les connexions entre les réseaux non approuvés et tous les composants du système dans l'environnement des données de titulaire de carte.</p> <p><i>Remarque : Un « réseau non approuvé » est tout réseau externe aux réseaux appartenant à l'entité sous investigation et/ou qui n'est pas sous le contrôle ou la gestion de l'entité.</i></p>	<p>Il est essentiel d'installer une protection réseau, en l'occurrence un pare-feu, entre le réseau approuvé interne et tout autre réseau non approuvé externe et/ou échappant au contrôle ou à la gestion de l'entité. Si cette protection n'est pas correctement mise en place, le réseau de l'entité sera exposé aux risques d'intrusion d'individus ou de logiciels malveillants.</p> <p>Si un pare-feu est installé mais n'intègre pas de règles contrôlant ou restreignant certains trafics, des individus malveillants pourront toujours exploiter les protocoles et les ports vulnérables pour attaquer votre réseau.</p>
<p>1.2.1 Restreindre le trafic entrant et sortant au trafic nécessaire à l'environnement des données de titulaire de carte</p>	<p>Cette exigence vise à empêcher des individus malveillants d'accéder au réseau de l'entreprise par le biais d'adresses IP non autorisées ou d'utiliser des services, des protocoles ou des ports de manière non autorisée (par exemple, pour transmettre les données obtenues au sein de votre réseau vers un serveur non approuvé).</p> <p>Tous les pare-feu doivent comprendre une règle qui refuse tout trafic entrant ou sortant qui n'est pas spécifiquement requis. Cela évitera les failles accidentelles susceptibles de permettre les trafics malveillants, indésirables et autres en entrée ou en sortie.</p>
<p>1.2.2 Sécuriser et synchroniser les fichiers de configuration des routeurs</p>	<p>Alors que les fichiers de configuration d'exécution sont généralement implémentés avec des paramètres sécurisés, il est possible que les fichiers de démarrage (les routeurs n'exécutent ces fichiers qu'au redémarrage) ne soient pas implémentés avec ces mêmes paramètres sécurisés du fait qu'ils ne s'exécutent qu'occasionnellement. Si un routeur redémarre sans les mêmes paramètres sécurisés que ceux définis dans les fichiers de configuration d'exécution, il peut en résulter un affaiblissement des règles dont un individu malveillant peut profiter pour s'introduire dans le réseau.</p>
<p>1.2.3 Installer des pare-feu de périmètre entre tous les réseaux sans fil et l'environnement des données de titulaire de carte, et configurer ces pare-feu pour refuser ou contrôler le trafic (si celui-ci est nécessaire à des fins professionnelles)</p>	<p>L'implémentation et l'exploitation connues (ou inconnues) de la technologie sans fil sur un réseau sont souvent mises à profit par les individus malveillants pour accéder au réseau et aux données de titulaire de carte. Si un périphérique ou un réseau sans fil est installé à l'insu d'une entreprise, un individu malveillant pourrait facilement, et à l'insu de tous, s'introduire dans le réseau. Si les pare-feu ne restreignent pas l'accès à l'environnement des cartes de paiement à partir des réseaux sans fil, les individus malveillants qui accèdent au réseau sans fil sans autorisation peuvent facilement se connecter à cet environnement et compromettre les informations de comptes.</p>

Exigence	Directive
<p>1.3 Interdire l'accès public direct entre Internet et tout composant du système dans l'environnement des données de titulaire de carte</p>	<p>Un pare-feu sert à gérer et contrôler toutes les connexions entre les systèmes publics et les systèmes internes (en particulier ceux qui stockent les données de titulaire de carte). Si un accès direct est autorisé entre les systèmes publics et ceux qui stockent les données de titulaire de carte, les protections offertes par le pare-feu sont ignorées et les composants du système stockant les données de titulaire de carte peuvent s'en trouver compromis.</p>
<p>1.3.1 Déployer une zone démilitarisée pour limiter le trafic entrant et sortant aux seuls protocoles nécessaires à l'environnement des données de titulaire de carte</p>	<p>Ces exigences visent à empêcher les individus malveillants d'accéder au réseau de l'entreprise par le biais d'adresses IP non autorisées ou en utilisant des services, des protocoles ou des ports de manière non autorisée (par exemple, pour transmettre les données obtenues au sein de votre réseau vers un serveur externe non approuvé sur un réseau non approuvé).</p>
<p>1.3.2 Limiter le trafic Internet entrant aux adresses IP dans la zone démilitarisée</p>	
<p>1.3.3 N'autoriser aucun acheminement direct entrant ou sortant du trafic entre Internet et l'environnement des données de titulaire de carte</p>	<p>La zone démilitarisée est la partie du pare-feu qui est tournée vers le réseau Internet public et qui gère les connexions entre Internet et les services internes qu'une entreprise doit mettre à la disposition du public (par exemple, un serveur Web). Il s'agit de la première ligne de défense dans l'isolation et la séparation du trafic qui doit communiquer avec le réseau interne des autres trafics.</p>
<p>1.3.4 Ne pas autoriser le passage des adresses internes d'Internet dans la zone démilitarisée</p>	<p>Un paquet contient normalement l'adresse IP de l'ordinateur qui l'envoie initialement. Les autres ordinateurs connectés au réseau peuvent ainsi identifier l'origine du paquet. Dans certains cas, cette adresse IP expéditrice est usurpée par des individus malveillants.</p> <p>Par exemple, ceux-ci peuvent envoyer un paquet à partir d'une fausse adresse de sorte qu'il parvienne à votre réseau depuis Internet, tout en semblant interne, et donc, légitime (à moins que votre pare-feu ne l'interdise). Une fois que l'individu malveillant a accédé à votre réseau, il peut commencer à compromettre vos systèmes.</p> <p>Le filtrage d'entrée est une technique que vous pouvez utiliser sur votre pare-feu pour filtrer les paquets entrants sur votre réseau afin de veiller, entre autres, à ce qu'ils ne soient pas falsifiés pour sembler provenir de votre propre réseau interne. Pour plus d'informations sur le filtrage des paquets, envisager d'obtenir des informations sur une technique corollaire appelée « filtrage de sortie ».</p>
<p>1.3.5 Restreindre le trafic sortant de l'environnement des données de titulaire de carte vers Internet de sorte que ce trafic ne puisse accéder qu'aux adresses IP dans la zone démilitarisée</p>	<p>La zone démilitarisée devrait également évaluer l'ensemble du trafic sortant sur le réseau afin de s'assurer qu'il est conforme aux règles définies. Pour que la zone démilitarisée remplisse cette fonction de manière efficace, les connexions du réseau vers toute adresse extérieure ne devraient pas être autorisées à moins qu'elles ne passent au préalable par la zone démilitarisée, qui en évaluera la légitimité.</p>

Exigence	Directive
<p>1.3.6 Implémenter le contrôle avec état, également appelé « filtrage des paquets dynamique » (seules les « connexions établies » sont autorisées sur le réseau).</p>	<p>Un pare-feu qui effectue un contrôle des paquets avec état maintient « l'état » (ou le statut) de chaque connexion au pare-feu. En maintenant « l'état », le pare-feu sait si ce qui semble être une réponse à une connexion antérieure est véritablement une réponse (puisqu'il « mémorise » la connexion antérieure) ou s'il s'agit d'un individu malveillant ou d'un logiciel malicieux qui essaie de le tromper pour autoriser la connexion.</p>
<p>1.3.7 Placer la base de données dans une zone de réseau interne, isolée de la zone démilitarisée.</p>	<p>Les données de titulaire de carte exigent le niveau de protection des informations le plus élevé. Si les données de titulaire de carte se trouvent dans la zone démilitarisée, un pirate externe peut plus facilement y accéder puisqu'il y a moins de couches à pénétrer.</p>
<p>1.3.8 Appliquer des masques IP pour empêcher la conversion des adresses internes et leur divulgation sur Internet, à l'aide de l'espace d'adresse RFC 1918. Utiliser des technologies de traduction d'adresses réseau (NAT, Network Address Translation), par exemple, la traduction d'adresses de ports (PAT, Port Address Translation).</p>	<p>Les masques IP, qui sont gérés par le pare-feu, permettent à une entreprise d'avoir des adresses internes qui sont uniquement visibles au sein du réseau, et des adresses externes qui sont visibles depuis l'extérieur. Si un pare-feu ne masque pas les adresses IP du réseau interne, un individu malveillant pourrait découvrir les adresses IP internes et tenter d'accéder au réseau au moyen d'une fausse adresse IP.</p>
<p>1.4 Installer un logiciel pare-feu personnel sur tout ordinateur portable et/ou ordinateur appartenant à un employé équipé d'une connexion directe à Internet (par exemple, ordinateurs portables utilisés par les employés), qui est utilisé pour accéder au réseau de l'entreprise.</p>	<p>Si un ordinateur n'est pas doté d'un pare-feu ou d'un programme antivirus, des logiciels espions (spyware), des chevaux de Troie, des virus, des vers et des dissimulateurs d'activités (programmes malveillants) peuvent être téléchargés et/ou installés à l'insu de tous. L'ordinateur est encore plus vulnérable lorsqu'il est directement connecté à Internet et n'est pas protégé par le pare-feu de l'entreprise. Lorsque l'ordinateur est reconnecté au réseau de l'entreprise, les programmes malveillants chargés sur l'ordinateur pendant qu'il n'était pas protégé par le pare-feu peuvent alors cibler malicieusement les informations sur le réseau.</p>

Exigence 2 : Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur

Les individus malveillants, qu'ils soient à l'intérieur ou à l'extérieur d'une entreprise, utilisent souvent les mots de passe et autres paramètres par défaut définis par le fournisseur pour s'infiltrer dans les systèmes en vue de les endommager. Ces mots de passe et paramètres sont bien connus des communautés de pirates et sont facilement détectables à partir d'informations publiques.

Exigence	Directive
<p>2.1 Changer systématiquement les paramètres par défaut définis par le fournisseur avant d'installer un système sur le réseau ; par exemple, inclure des mots de passe et des chaînes de communauté SNMP (Simple Network Management Protocol), et éliminer les comptes qui ne sont pas nécessaires.</p>	<p>Les individus malveillants, qu'ils soient à l'intérieur ou à l'extérieur d'une entreprise, utilisent souvent les paramètres, les noms de comptes et les mots de passe par défaut définis par le fournisseur pour s'infiltrer dans les systèmes en vue de les endommager. Ces paramètres sont bien connus des communautés de pirates et exposent considérablement votre système à des risques d'attaques.</p>
<p>2.1.1 Pour les environnements sans fil connectés à l'environnement des données de titulaire de carte ou la transmission de données de titulaire de carte, modifier les paramètres par défaut définis par le fournisseur des équipements sans fil, notamment les mots de passe, les chaînes de communauté SNMP et les clés de cryptage sans fil par défaut. Vérifier que les paramètres de sécurité des périphériques sans fil sont activés afin d'appliquer un cryptage robuste aux fonctionnalités d'authentification et de transmission.</p>	<p>De nombreux utilisateurs installent ces équipements sans l'approbation de la direction et ne modifient pas les paramètres par défaut, ni ne configurent des paramètres de sécurité. Si la sécurité des réseaux sans fil déployés n'est pas suffisante (y compris par la modification des paramètres par défaut), des renifleurs sans fil peuvent intercepter le trafic, capturer facilement les données et les mots de passe, et pénétrer sans encombre dans votre réseau en vue de l'attaquer. En outre, le protocole d'échange de clés de l'ancienne version du cryptage 802.11x (WEP) a été décrypté et peut rendre le cryptage inutile. Vérifiez que le firmware des équipements est mis à jour pour prendre en charge des protocoles plus sécurisés tels que WPA/WPA2.</p>

Exigence	Directive
<p>2.2 Élaborer des normes de configuration pour tous les composants du système. S'assurer que ces normes couvrent toutes les vulnérabilités de la sécurité et sont compatibles avec toutes les normes renforçant les systèmes en vigueur dans le secteur.</p>	<p>De nombreux systèmes d'exploitation, bases de données et applications d'entreprise présentent des points faibles connus et les moyens de les configurer pour résoudre les vulnérabilités en matière de sécurité sont également connus. Pour aider les utilisateurs non expérimentés en matière de sécurité, les entreprises de sécurité ont défini des recommandations visant à renforcer les systèmes, qui vous indiquent comment corriger ces failles. Si les systèmes sont laissés en l'état, par exemple avec des paramètres de fichier faibles ou des services et des protocoles par défaut (services ou protocoles qui sont souvent superflus), un pirate pourra exploiter les nombreuses failles connues pour attaquer les services et protocoles vulnérables, et accéder ainsi au réseau de votre entreprise. Visitez les trois sites Web indiqués ci-dessous à titre d'exemple pour en savoir plus sur les meilleures pratiques du secteur qui vous aideront à mettre en œuvre les normes de configuration : www.nist.gov, www.sans.org, www.cisecurity.org</p>
<p>2.2.1 Implémenter une seule fonction principale par serveur.</p>	<p>Cette condition vise à ce que les normes de configuration et les processus associés de votre entreprise prennent en charge les fonctions d'un serveur qui doivent avoir différents niveaux de sécurité, ou qui introduisent des vulnérabilités en matière de sécurité d'autres fonctions sur le même serveur. Par exemple :</p> <ol style="list-style-type: none"> 1. une base de données, qui doit être dotée de stratégies de sécurité robustes, serait exposée à des risques si elle partageait un serveur avec une application Web, qui doit être ouvert et directement tourné vers Internet. 2. La non-application d'un correctif à une fonction en apparence mineure peut entraîner des risques qui affectent d'autres fonctions bien plus importantes (comme une base de données) sur le même serveur. <p>Cette exigence concerne les serveurs (généralement Unix, Linux ou Windows), mais pas les systèmes mainframe.</p>
<p>2.2.2 Désactiver tous les services et protocoles non sécurisés et non requis (services et protocoles qui ne sont pas directement nécessaires pour exécuter la fonction spécifiée du périphérique).</p>	<p>Comme indiqué au point 1.1.7, une entreprise peut avoir besoin de nombreux protocoles (ou ceux-ci peuvent être activés par défaut) qui sont fréquemment utilisés par les individus malveillants pour accéder à un réseau en vue de l'endommager. Pour veiller à ce que ces services et protocoles soient toujours désactivés lors du déploiement de nouveaux serveurs, cette exigence doit faire partie des normes de configuration et processus associés de votre entreprise.</p>

Exigence	Directive
<p>2.2.3 Configurer les paramètres de sécurité du système pour empêcher les actes malveillants.</p>	<p>Cette condition vise à ce que les normes de configuration et les processus associés de votre entreprise prennent en charge les paramètres de sécurité et les configurations impliquant des risques connus en termes de sécurité.</p>
<p>2.2.4 Supprimer toutes les fonctionnalités qui ne sont pas nécessaires, par exemple scripts, pilotes, fonctions, sous-systèmes, systèmes de fichiers et serveurs Web superflus.</p>	<p>Les normes renforçant les serveurs doivent inclure des processus prenant en charge les fonctionnalités impliquant des risques spécifiques en termes de sécurité (par exemple, la suppression/désactivation de la fonction FTP ou du serveur Web si le serveur n'exécute pas ces fonctions).</p>
<p>2.3 Crypter tous les accès administratifs non-console Utiliser des technologies telles que SSH, VPN ou SSL/TLS pour la gestion via le Web et autres accès administratifs non-console.</p>	<p>Si l'administration à distance ne repose pas sur une authentification sécurisée et des communications cryptées, les données au niveau opérationnel ou les informations administratives sensibles (comme les mots de passe de l'administrateur) peuvent être interceptées. Un individu malveillant peut alors utiliser ces informations pour accéder au réseau, se substituer à l'administrateur et subtiliser des données.</p>
<p>2.4 Les fournisseurs d'hébergement partagé doivent protéger l'environnement hébergé et les données de chaque entité. Ces fournisseurs doivent satisfaire aux exigences spécifiques décrites dans l'<i>annexe A : Autres exigences des normes PCI DSS s'appliquant aux fournisseurs d'hébergement partagé.</i></p>	<p>Cette condition s'applique aux fournisseurs d'hébergement qui proposent des environnements d'hébergement partagé à plusieurs clients sur le même serveur. Lorsque toutes les données se trouvent sur le même serveur et sont contrôlées par un environnement unique, les paramètres des serveurs partagés ne sont généralement pas gérables par les différents clients, ils permettent aux clients d'ajouter des fonctions et des scripts non sécurisés susceptibles d'affecter la sécurité des environnements de tous les autres clients et, par conséquent, ils facilitent l'accès d'un individu malveillant aux données d'un client, et de tous les autres clients, en vue de les endommager. Voir l'annexe A.</p>

Directives relatives aux exigences 3 et 4 : Protection des données de titulaire de carte de crédit

Exigence 3 : Protéger les données de titulaire de carte stockées

Les mesures de protection, telles que le cryptage, la troncature, le masquage et le hachage, sont des composants stratégiques de la protection des données de titulaire de carte. Si un intrus parvient à contourner les autres contrôles de sécurité réseau et à accéder aux données cryptées, il ne pourra pas les lire ni les utiliser s'il n'a pas les clés cryptographiques appropriées. D'autres méthodes efficaces de protection des données stockées doivent être envisagées pour limiter les risques. Par exemple, pour minimiser les risques, vous devez éviter de stocker les données de titulaire de carte à moins que cela ne soit absolument nécessaire, tronquer les données de titulaire de carte si un PAN complet n'est pas requis et éviter d'envoyer un PAN dans des e-mails non cryptés.

Pour obtenir la définition d'une « cryptographie robuste » et d'autres termes relatifs à PCI DSS, consultez le Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS.

Exigence	Directive
3.1 Stocker les données de titulaire de carte le moins possible. Développer une politique de conservation et d'élimination des données. Limiter la quantité des données stockées et les délais de conservation aux conditions requises par l'entreprise, la loi et/ou les réglementations, comme décrit dans la politique de conservation des données.	Le stockage de trop nombreuses données de titulaire de carte, au-delà des besoins de l'entreprise, entraîne des risques superflus. Les seules données de titulaire de carte qui doivent être stockées sont le PAN (Primary Account Number ou numéro de compte principal), rendu illisible, la date d'expiration, le nom du titulaire et le code de service. Ne stockez pas les informations dont vous n'avez pas besoin !
3.2 Ne stocker aucune donnée d'authentification sensible après autorisation (même cryptée). Les données concernées sont mentionnées dans les exigences 3.2.1 à 3.2.3 suivantes :	Les données d'authentification sensibles comprennent les données de la bande magnétique (ou piste) ⁷ , le code ou la valeur de validation de carte ⁸ et le code PIN ⁹ . Le stockage des données d'authentification sensibles après autorisation est interdit ! Ces données sont très utiles aux individus malveillants car elles leur permettent de créer de fausses cartes de paiement et des transactions frauduleuses. Voir la définition intégrale des « données d'authentification sensibles » dans le <i>Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS</i> .

⁷ Données encodées sur la bande magnétique utilisée pour une autorisation lors d'une transaction carte présente. Ces données peuvent également se trouver dans l'image de la bande magnétique sur la puce ou sur un autre support de la carte. Les entités ne doivent pas conserver l'ensemble des données sur bande magnétique après l'autorisation des transactions. Les seuls éléments des données de piste pouvant être conservés sont le PAN, le nom du titulaire de carte, la date d'expiration et le code de service.

⁸ La valeur à trois ou quatre chiffres imprimée à droite de l'espace dédié à la signature ou sur la face d'une carte de paiement, utilisée pour vérifier les transactions carte absente.

⁹ Les données PIN (Personal Identification Number, numéro d'identification personnel) saisies par le titulaire de la carte lors d'une transaction carte présente et/ou le bloc PIN crypté présent dans le message de la transaction.

Exigence	Directive
<p>3.2.1 Ne jamais stocker la totalité du contenu d'une quelconque piste de la bande magnétique (au verso d'une carte, sur une puce ou ailleurs). Ces données sont également désignées par les termes « piste complète », « piste », « piste 1 », « piste 2 » et « données de bande magnétique ».</p> <p><i>Remarque : Dans le cadre normal de l'activité, il est parfois nécessaire de conserver les éléments de données de la bande magnétique ci-après :</i></p> <ul style="list-style-type: none"> ▪ le nom du titulaire de la carte ; ▪ le numéro de compte principal (PAN, Primary Account Number) ; ▪ la date d'expiration ; ▪ le code de service. <p><i>Afin de réduire le risque autant que possible, stocker uniquement les éléments de données nécessaires à l'activité.</i></p> <p><i>Remarque : Pour plus d'informations, se reporter au Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS.</i></p>	<p>Si les données de piste complètes sont stockées, les individus malveillants qui parviennent à se les procurer pourront les reproduire et vendre des cartes de paiement à travers le monde.</p>
<p>3.2.2 Ne pas stocker le code ou la valeur de validation de carte (nombre à trois ou quatre chiffres figurant au recto ou au verso de la carte de paiement), utilisé pour vérifier les transactions carte absente.</p> <p><i>Remarque : Pour plus d'informations, se reporter au Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS.</i></p>	<p>Le code de validation des cartes sert à protéger les transactions « carte absente », à savoir les transactions effectuées via Internet ou les ordres de paiement par e-mail/téléphone (MOTO), qui impliquent l'absence du consommateur et de la carte. Ces types de transactions ne peuvent être authentifiés comme émanant du titulaire de la carte qu'en demandant ce code de validation de carte, puisque le titulaire a la carte en main et peut lire ce code. Si ces données sont stockées en dépit de l'interdiction et venaient à être subtilisées, des individus malveillants pourraient exécuter des transactions MOTO et via Internet frauduleuses.</p>
<p>3.2.3 Ne pas stocker de code PIN (Personal Identification Number) ou de bloc PIN crypté.</p>	<p>Ces valeurs ne doivent être connues que du titulaire de la carte ou de la banque qui a émis la carte. Si ces données sont stockées en dépit de l'interdiction et venaient à être subtilisées, des individus malveillants pourraient exécuter des transactions de débit à l'aide du code PIN (par exemple, retraits au distributeur).</p>

Exigence	Directive
<p>3.3 Masquer le PAN lorsqu'il s'affiche (les six premiers chiffres et les quatre derniers sont le maximum de chiffres affichés).</p> <p><i>Remarques :</i></p> <ul style="list-style-type: none"> ▪ <i>Cette exigence ne s'applique pas aux employés et autres parties qui ont un besoin spécifique de voir l'intégralité du PAN.</i> ▪ <i>Cette exigence ne se substitue pas aux exigences plus strictes qui sont en place et qui régissent l'affichage des données de titulaire de carte, par exemple, pour les reçus des points de vente (POS).</i> 	<p>L'affichage du PAN complet, par exemple sur un écran d'ordinateur, un reçu de carte de paiement, un fax ou un rapport sur papier, peut entraîner la divulgation de cette information à des individus non autorisés et son exploitation frauduleuse. Le PAN peut être indiqué dans son intégralité sur la copie des reçus de paiement destinée au commerçant. Toutefois, ces reçus papier doivent être soumis aux mêmes règles de sécurité que les copies électroniques et doivent adhérer aux instructions des normes PCI DSS, en particulier l'exigence 9 relative à la sécurité physique. Le PAN complet peut aussi être visible aux utilisateurs qui ont un besoin professionnel légitime de le connaître.</p>
<p>3.4 Rendre le PAN au minimum illisible où qu'il soit stocké (y compris les données sur support numérique portable, support de sauvegarde, journaux), en utilisant l'une des approches suivantes :</p>	<p>En l'absence de protection adéquate des PAN, des individus malveillants risquent de les voir ou de les télécharger. Les PAN stockés sur les supports de stockage principal (par exemple, bases de données ou fichiers plats tels que des feuilles de calcul) et autres supports secondaires (sauvegardes ou journaux d'audit, d'exceptions ou de dépannage) doivent tous être protégés. Les dégâts résultant du vol ou de la perte des bandes de sauvegarde pendant le transport peuvent être réduits en veillant à ce que les PAN soient rendus illisibles par le cryptage, la troncature ou le hachage. Dans la mesure où les journaux d'audit, de dépannage et d'exceptions doivent être conservés, vous pouvez empêcher la divulgation de leurs contenus en y rendant les PAN illisibles (ou en les supprimant ou en les masquant). Pour obtenir la définition d'une « cryptographie robuste », consultez le <i>Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS</i>.</p>
<ul style="list-style-type: none"> ▪ Hachage unilatéral s'appuyant sur une méthode cryptographique robuste 	<p>Les fonctions de hachage unilatéral (telles que SHA-1) reposant sur une cryptographie robuste peuvent être utilisées pour rendre les données de titulaire de carte illisibles. Le recours à ces fonctions est approprié lorsqu'il n'est pas nécessaire de récupérer le numéro d'origine (le hachage unilatéral est irréversible).</p>
<ul style="list-style-type: none"> ▪ Troncature 	<p>La troncature vise à ce qu'une partie seulement (qui ne doit pas dépasser les six premiers et les quatre derniers chiffres) du PAN soit stockée. Cette méthode est différente du masquage, qui implique le stockage du PAN complet mais son masquage lorsqu'il est affiché (en d'autres termes, une partie seulement du PAN est révélée à l'écran, dans les rapports, les reçus, etc.).</p>

Exigence	Directive
<ul style="list-style-type: none"> ▪ Index tokens et Index pads (les pads doivent être stockés de manière sécurisée) 	<p>Il est également possible d'utiliser des Index tokens et des Index pads pour rendre les données de titulaire de carte illisibles. Un Index token est un jeton cryptographique qui remplace le PAN basé sur un indice donné par une valeur imprévisible. Un pad ponctuel est un système dans lequel une clé privée, générée de façon aléatoire, est utilisée une seule fois pour crypter un message qui est ensuite décrypté à l'aide d'un pad et d'une paire ponctuelle composée d'une clé et du pad correspondant.</p>
<ul style="list-style-type: none"> ▪ Cryptographie robuste associée à des processus et des procédures de gestion des clés. <p><i>En ce qui concerne les coordonnées de compte, au MINIMUM, le PAN doit être rendu illisible.</i></p> <p><i>Remarques :</i></p> <ul style="list-style-type: none"> ▪ <i>Si, pour quelque raison que ce soit, une société ne peut pas rendre le PAN illisible, voir l'annexe B: Contrôles compensatoires.</i> ▪ <i>Le terme « cryptographie robuste » est défini dans le Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS.</i> 	<p>La cryptographie robuste (voir la définition et les longueurs de clé dans le <i>Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS</i>) vise à ce que le cryptage repose sur un algorithme testé et accepté par le secteur (et non un algorithme propriétaire ou « développé en interne »).</p>
<p>3.4.1 Si un cryptage par disque est utilisé (au lieu d'un cryptage de base de données au niveau fichier ou colonne), l'accès logique doit être géré indépendamment des mécanismes de contrôle d'accès au système d'exploitation natif (par exemple, en n'utilisant pas des bases de données de comptes d'utilisateur locales). Les clés de décryptage ne doivent pas être liées à des comptes d'utilisateur.</p>	<p>Cette exigence porte sur l'acceptabilité du cryptage par disque pour rendre les données de titulaire de carte illisibles. Cette méthode crypte les données stockées sur le volume de stockage de masse d'un ordinateur et décrypte automatiquement les informations à la demande d'un utilisateur autorisé. Les systèmes de cryptage par disque interceptent les opérations de lecture et d'écriture du système d'exploitation et exécutent les transformations cryptographiques appropriées sans aucune action particulière de l'utilisateur autre que la saisie d'un mot de passe au début d'une session. Compte tenu de ces caractéristiques du cryptage par disque, pour être conforme à cette exigence, la méthode de cryptage par disque ne peut pas avoir :</p> <ol style="list-style-type: none"> 1) une association directe avec le système d'exploitation, ou 2) des clés de décryptage associées à des comptes d'utilisateur.

Exigence	Directive
3.5 Protéger les clés de cryptage utilisées pour le cryptage des données de titulaire de carte contre la divulgation et l'utilisation illicite.	Les clés cryptographiques doivent être bien protégées, car tout individu qui parviendrait à se les procurer pourra décrypter les données.
3.5.1 Restreindre l'accès aux clés cryptographiques au plus petit nombre d'opérateurs possible.	Peu de personnes devraient avoir accès aux clés cryptographiques. Généralement, seuls les opérateurs chargés de la gestion de ces clés devraient pouvoir y accéder.
3.5.2 Stocker les clés cryptographiques de manière sécurisée dans aussi peu d'emplacements et de formes que possible.	Les clés cryptographiques doivent être stockées de manière sécurisée. Elles doivent généralement être cryptées à l'aide de clés de cryptage de clés et stockées en peu d'endroits.
3.6 Documenter en détail et déployer les processus et les procédures de gestion des clés cryptographiques servant au cryptage des données de titulaire de carte, notamment ce qui suit :	La manière dont les clés cryptographiques sont gérées est un pan essentiel de la sécurité permanente de la solution de cryptage. Un processus de gestion des clés adéquats, qu'il soit manuel ou automatique dans le cadre du logiciel de cryptage, prend en charge tous les éléments clés décrits au point 3.6.1 à 3.6.8.
3.6.1 Génération de clés cryptographiques robustes	La solution de cryptage doit générer des clés indécryptables, comme défini à l'entrée « cryptographie robuste » dans le <i>Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS</i> .
3.6.2 Sécuriser la distribution des clés cryptographiques	La solution de cryptage doit distribuer les clés de manière sécurisée. En d'autres termes, les clés ne sont pas distribuées en texte clair et elles ne sont communiquées qu'aux opérateurs chargés de leur gestion, identifiés au point 3.5.1.
3.6.3 Sécuriser le stockage des clés cryptographiques	La solution de cryptage doit stocker les clés de manière sécurisée. En d'autres termes, les clés ne sont pas stockées en texte clair (elles doivent être cryptées à l'aide d'une clé de cryptage de clés).
3.6.4 Modification périodique des clés cryptographiques <ul style="list-style-type: none"> • Comme cela est jugé nécessaire et recommandé par l'application associée (par exemple, recomposition), de préférence automatiquement • Au moins une fois par an 	Suivez tous les processus ou recommandations de changement de clés régulier éventuellement spécifiés par le fournisseur de l'application de cryptage. Il est impératif de changer les clés de cryptage une fois par an afin de réduire les risques qu'un tiers se les procure et ne parvienne à décrypter les données.

Exigence	Directive
<p>3.6.5 Retrait ou remplacement des clés cryptographiques obsolètes ou soupçonnées d'avoir été compromises</p>	<p>Les clés obsolètes, qui ne sont plus utilisées ou requises, doivent être supprimées et détruites afin de veiller à ce qu'elles ne puissent plus servir. Si les anciennes clés doivent être conservées (par exemple, pour permettre l'accès à des données cryptées archivées), elles doivent être bien protégées. (Voir le point 3.6.6 ci-dessous.) La solution de cryptage doit également prévoir un processus de remplacement des clés dont on sait, ou dont on soupçonne, qu'elles sont compromises.</p>
<p>3.6.6 Fractionner les connaissances et l'établissement d'un double contrôle des clés cryptographiques</p>	<p>Le fractionnement des connaissances et le double contrôle des clés sont utilisés pour éliminer la possibilité qu'une seule personne puisse accéder à l'intégralité d'une clé. Ce contrôle s'applique généralement aux systèmes de cryptage des clés manuels ou si la gestion des clés n'est pas implémentée par la solution de cryptage. Ce type de contrôle est généralement mis en œuvre dans le cadre de modules de sécurité matériels.</p>
<p>3.6.7 Empêcher la substitution non autorisée des clés cryptographiques</p>	<p>La solution de cryptage ne doit pas autoriser ni accepter la substitution de clés émanant de sources non autorisées ou de processus inattendus.</p>
<p>3.6.8 Exiger des opérateurs chargés de la gestion de clés cryptographiques de signer un formulaire reconnaissant qu'ils comprennent et acceptent leurs responsabilités</p>	<p>Ce processus garantit que l'individu s'engage à bien protéger les clés et comprend bien les responsabilités qui lui incombent.</p>

Exigence 4 : Crypter la transmission des données de titulaire de carte sur les réseaux publics ouverts

Les informations sensibles doivent être cryptées pendant leur transmission sur des réseaux accessibles à des individus malveillants. Les réseaux sans fil mal configurés et les vulnérabilités dans les protocoles traditionnels de cryptage et d'authentification peuvent être des cibles permanentes des individus malveillants qui profitent de ces faiblesses pour obtenir un accès privilégié aux environnements des données de titulaire de carte.

Exigence	Directive
<p>4.1 Utiliser des protocoles de cryptographie et de sécurité robustes, tels que SSL/TLS ou IPSEC pour sauvegarder les données de titulaire de carte sensibles lors de leur transmission sur des réseaux publics ouverts.</p> <p><i>Voici quelques exemples de réseaux publics ouverts couverts par les normes PCI DSS :</i></p> <ul style="list-style-type: none">▪ <i>Internet</i>▪ <i>Technologies sans fil</i>▪ <i>Communications GSM (Global Système for Mobile)</i>▪ <i>GPRS (General Packet Radio Service)</i>	<p>Les informations sensibles doivent être cryptées pendant leur transmission sur des réseaux publics, car il est facile et courant qu'un individu malveillant les intercepte et/ou les détourne pendant cette opération. Le protocole SSL (Secure Sockets Layer) crypte les pages Web et les données qui y sont saisies. Lors de l'utilisation de sites Web sécurisés à l'aide du protocole SSL, assurez-vous que « https » fasse partie de l'adresse URL.</p> <p>Notez que les versions du protocole SSL antérieures à la version 3.0 comprennent les vulnérabilités décrites, telles que la saturation de la mémoire tampon, qu'un pirate peut exploiter pour accéder au système concerné.</p>

Exigence	Directive
<p>4.1.1 S'assurer que les réseaux sans fil sur lesquels sont transmises les données de titulaire de carte ou qui sont connectés à l'environnement des données de titulaire de carte mettent en œuvre les meilleures pratiques du secteur (par exemple, IEEE 802.11i) pour appliquer un cryptage robuste pour l'authentification et la transmission.</p> <ul style="list-style-type: none"> ▪ <i>Dans le cadre des nouveaux déploiements sans fil, la mise en œuvre du protocole WEP est interdite à compter du 31 mars 2009.</i> ▪ <i>Dans le cadre des déploiements actuels, la mise en œuvre du protocole WEP est interdite après le 30 juin 2010.</i> 	<p>Les utilisateurs malveillants emploient des outils gratuits et très répandus pour écouter les communications sans fil. L'utilisation de la méthode de cryptage appropriée peut empêcher ces écoutes et la divulgation d'informations sensibles sur le réseau. Dans de nombreux cas connus, des utilisateurs malveillants ont accédé aux données de titulaire de carte stockées exclusivement sur le réseau câblé à partir d'un réseau sans fil non sécurisé.</p> <p>Un cryptage robuste pour l'authentification et la transmission des données de titulaire de carte est requis pour empêcher les utilisateurs malveillants d'accéder au réseau sans fil, et donc aux données stockées dessus, ou d'utiliser les réseaux sans fil pour accéder à d'autres données ou réseaux internes. Le protocole WEP n'utilise pas un cryptage robuste. Le cryptage WEP ne doit jamais être employé seul puisqu'il est vulnérable en raison de la faiblesse des vecteurs initiaux (IV) dans le processus d'échange de clés WEP et de l'absence de la rotation des clés requise. Un pirate peut utiliser les outils d'attaque par force brute, disponibles gratuitement, pour décrypter le cryptage WEP.</p> <p>Les dispositifs sans fil actuels doivent être mis à niveau (par ex. : mettez à niveau le firmware des points d'accès vers WPA) pour prendre en charge le cryptage robuste. Si les dispositifs actuels ne peuvent pas être mis à niveau, vous devez acheter de nouveaux équipements.</p> <p>Si les réseaux sans fil utilisent le cryptage WEP, ils ne devraient pas avoir accès aux environnements des données de titulaire de carte.</p>
<p>4.2 Ne jamais envoyer de PAN non cryptés à l'aide de technologies de messagerie pour les utilisateurs finaux (par exemple e-mail, messagerie instantanée, chat).</p>	<p>La messagerie électronique, la messagerie instantanée et le chat peuvent être facilement interceptés par un renifleur de paquets pendant les échanges sur les réseaux internes et publics. N'envoyez jamais de PAN à l'aide de ces outils de messagerie à moins qu'ils n'intègrent des fonctions de cryptage.</p>

Directives relatives aux exigences 5 et 6 : Gestion d'un programme de gestion des vulnérabilités

Exigence 5 : Utiliser des logiciels antivirus et les mettre à jour régulièrement

Des logiciels malicieux, généralement appelés « programmes malveillants », par exemple virus, vers et chevaux de Troie, sont infiltrés dans le réseau dans le cadre d'activités professionnelles approuvées, notamment l'échange d'e-mails et l'accès à Internet des employés ainsi que l'utilisation de périphériques de stockage et d'ordinateurs portables. Les vulnérabilités des systèmes peuvent alors être exploitées à des fins malveillantes. Des logiciels antivirus doivent être installés sur tous les systèmes régulièrement affectés par des programmes malveillants afin de les protéger contre les menaces logicielles actuelles et futures.

Exigence	Directive
<p>5.1 Déployer des logiciels antivirus sur tous les systèmes régulièrement affectés par des logiciels malveillants (en particulier PC et serveurs).</p>	<p>Un type d'attaque très courant repose sur les codes d'exploitation publiés à grande échelle, souvent de type « 0 jour » (ou 0 day) (codes d'exploitation publiés et diffusés sur les réseaux une heure après leur découverte), contre des systèmes sécurisés. En l'absence de logiciels antivirus régulièrement mis à jour, ces nouvelles formes de logiciels malicieux peuvent attaquer votre réseau et le mettre hors service.</p> <p>Les logiciels malicieux peuvent être téléchargés et/ou installés depuis Internet à votre insu. Toutefois, les ordinateurs sont également vulnérables lors de l'utilisation de périphériques de stockage amovibles, tels que CD et DVD, disques durs et clés USB, appareils photo numériques, assistants numériques personnels (PDA) et autres périphériques. En l'absence de logiciels antivirus, ces ordinateurs peuvent devenir des points d'accès à votre réseau et/ou cibler à des fins malveillantes les informations disponibles sur le réseau.</p> <p>Bien que les systèmes généralement touchés par les logiciels malicieux ne comprennent pas les systèmes mainframe et la plupart des systèmes Unix (voir ci-dessous pour plus d'informations), chaque entité doit disposer d'un processus conforme à l'exigence 6.2 des normes PCI DSS lui permettant d'identifier et de résoudre les nouvelles failles en matière de sécurité, et de mettre à jour ses processus et ses normes de configuration en conséquence. Les tendances liées aux logiciels malicieux qui affectent les systèmes d'exploitation utilisés par une entité doivent être inclus dans l'identification des nouvelles vulnérabilités en matière de sécurité et les méthodes de résolution correspondantes doivent être intégrées aux normes de configuration et aux mécanismes de protection de l'entreprise, comme requis.</p>

Exigence	Directive
	<p>Les systèmes d'exploitation ne sont généralement pas touchés par les logiciels malicieux : mainframe et certains serveurs Unix (tels qu'AIX, Solaris et HP-Unix). Toutefois, les tendances sectorielles liées aux logiciels malicieux peuvent changer rapidement et chaque entreprise doit se conformer à l'exigence 6.2 pour identifier et résoudre les nouvelles vulnérabilités en matière de sécurité, et mettre à jour ses processus et ses normes de configuration en conséquence.</p>
<p>5.1.1 S'assurer que tous les programmes antivirus sont capables de détecter et d'éliminer tous les types de logiciels malveillants connus, et de constituer une protection efficace contre ce fléau.</p>	<p>Il est important de se protéger contre TOUS les types et formes de logiciels malicieux.</p>
<p>5.2 S'assurer que tous les mécanismes antivirus sont à jour, en cours d'exécution et capables de générer des journaux d'audit.</p>	<p>L'efficacité des meilleurs logiciels antivirus est limitée si les signatures ne sont pas tenues à jour et si ces logiciels ne sont pas activés sur le réseau ou sur l'ordinateur d'un utilisateur. Les journaux d'audit permettent de surveiller l'activité des virus et les réactions antivirus.</p>

Exigence 6 : Développer et gérer des systèmes et des applications sécurisés

Des individus sans scrupules peuvent exploiter les points faibles de la sécurité pour obtenir un accès privilégié aux systèmes. Bon nombre de ces vulnérabilités sont résolues par les correctifs de sécurité développés par les fournisseurs. Ceux-ci doivent être installés par les entités chargées de la gestion des systèmes. Tous les systèmes stratégiques doivent être dotés des correctifs logiciels appropriés les plus récents afin d'empêcher l'exploitation et l'altération des données de titulaire de carte par des individus et des logiciels malveillants.

Remarque : Les correctifs logiciels appropriés sont ceux qui ont été suffisamment évalués et testés pour déterminer qu'ils ne présentent aucun conflit avec les configurations de sécurité existantes. De nombreuses vulnérabilités peuvent être évitées dans les applications développées en interne grâce à l'utilisation de processus de développement système standard et de techniques de codage sécurisées.

Exigence	Directive
<p>6.1 S'assurer que tous les logiciels et les composants du système sont dotés des derniers correctifs de sécurité développés par le fournisseur. Installer les correctifs de sécurité stratégiques dans le mois qui suit leur commercialisation.</p> <p><i>Remarque : Une entreprise peut envisager la mise en œuvre d'une approche en fonction du risque pour définir la priorité des correctifs à installer. Par exemple, en accordant aux infrastructures stratégiques (par exemple, bases de données, périphériques et systèmes orientés public) une priorité supérieure à celle des périphériques internes moins cruciaux, de sorte que les systèmes et les périphériques hautement prioritaires soient traités dans un délai d'un mois, tandis que les périphériques et systèmes moins stratégiques le soient dans un délai de trois mois.</i></p>	<p>Un grand nombre d'attaques repose sur les codes d'exploitation publiés à grande échelle, souvent de type « 0 jour » (ou 0 day) (codes d'exploitation publiés une heure après leur découverte), contre des systèmes sécurisés. Si les correctifs les plus récents ne sont pas installés sur les systèmes stratégiques dans les plus brefs délais, un individu malveillant peut utiliser des codes d'exploitation pour attaquer le réseau et le mettre hors service. Envisagez de définir la priorité des changements à effectuer. Par exemple, vous pouvez installer les correctifs de sécurité cruciaux sur les systèmes stratégiques ou exposés à des risques dans un délai de 30 jours et vous occuper des changements impliquant des risques moindres dans un délai de deux à trois mois.</p>
<p>6.2 Définir un processus d'identification des nouvelles vulnérabilités de la sécurité (par exemple, abonnement à des services de notification gratuits sur Internet). Mettre à jour les normes de configuration comme stipulé par l'exigence 2.2 des normes PCI DSS afin de résoudre les nouvelles vulnérabilités.</p>	<p>Cette exigence vise à ce que les entreprises soient tenues au courant des nouvelles vulnérabilités afin de pouvoir protéger leurs réseaux de manière appropriée et d'incorporer ces failles dans leurs normes de configuration.</p>

Exigence	Directive
<p>6.3 Développer des applications logicielles conformément aux normes PCI DSS (par exemple, authentification et connexion sécurisées) et sur la base des meilleures pratiques du secteur, et incorporer des informations sur la sécurité tout au long du cycle de développement des logiciels. Ces processus doivent inclure ce qui suit :</p>	<p>Si les questions liées à la sécurité ne sont pas prises en compte pendant les phases de définition des exigences, de conception, d'analyse et de test du développement de logiciels, des vulnérabilités en matière de sécurité peuvent être introduites, accidentellement ou de façon malveillante, dans l'environnement de production.</p>
<p>6.3.1 Tester tous les correctifs de sécurité, ainsi que toute modification de configuration de système ou de logiciel avant déploiement</p> <p>6.3.1.1 Validation de toutes les entrées (afin d'empêcher les attaques XSS (Cross-Site Scripting), les attaques par injection, l'exécution de fichier malveillant, etc.)</p> <p>6.3.1.2 Validation du traitement approprié des erreurs</p> <p>6.3.1.3 Validation du stockage cryptographique sécurisé</p> <p>6.3.1.4 Validation des communications sécurisées</p> <p>6.3.1.5 Validation du RBAC (Role-Based Access Control) approprié</p>	<p>Veillez à ce que toutes les installations et modifications soient effectuées comme prévu et qu'aucune fonction ne soit inattendue, indésirable ou nuisible.</p>
<p>6.3.2 Séparer les environnements de développement/test et de production.</p>	<p>Les environnements de développement et de test sont souvent moins sécurisés que l'environnement de production. Sans une séparation adéquate, l'environnement de production et les données de titulaire de carte peuvent être exposées à des risques en raison des vulnérabilités ou de la faiblesse des processus internes.</p>
<p>6.3.3 Séparer les obligations entre les environnements de développement/test et de production.</p>	<p>Cette séparation réduit au minimum le nombre d'employés qui ont accès à l'environnement de production et aux données de titulaire de carte, et contribue à s'assurer que l'accès est limité à ceux qui en ont vraiment besoin.</p>
<p>6.3.4 Les données de production (PAN actifs) ne sont pas utilisées à des fins de test ou de développement.</p>	<p>Les contrôles de sécurité ne sont généralement pas aussi stricts dans l'environnement de développement. L'utilisation des données de production permet aux individus malveillants d'accéder illicitement à ces informations (données de titulaire de carte).</p>

Exigence	Directive
<p>6.3.5 Suppression des données et des comptes de test avant que les systèmes de production ne deviennent actifs.</p>	<p>Les comptes et les données de test doivent être éliminés du code de production avant l'activation de l'application, puisque ces éléments peuvent divulguer des informations sur le fonctionnement de l'application. La possession de ces informations peut faciliter l'accès à l'application et aux données de titulaire de carte en vue de les endommager.</p>
<p>6.3.6 Suppression des comptes d'application personnalisés, des noms d'utilisateur et des mots de passe avant l'activation des applications ou leur mise à la disposition des clients.</p>	<p>Les comptes d'application personnalisés, les noms d'utilisateur et les mots de passe doivent être supprimés du code de production avant l'activation de l'application ou sa mise à la disposition des clients puisque ces éléments peuvent révéler des informations sur le fonctionnement de l'application. La possession de ces informations peut faciliter l'accès à l'application et aux données de titulaire de carte en vue de les endommager.</p>
<p>6.3.7 Examen du code personnalisé avant sa mise en production ou sa mise à la disposition des clients afin d'identifier toute vulnérabilité du codage éventuelle.</p> <p><i>Remarque : Cette exigence s'applique à l'intégralité du code personnalisé (aussi bien interne qu'orienté public), dans le cadre du cycle de développement du système défini par l'exigence 6.3 des normes PCI DSS. Les examens du code peuvent être réalisés par le personnel interne compétent. Les applications Web font également l'objet de contrôles supplémentaires si elles sont orientées public afin de résoudre les menaces et les vulnérabilités éventuelles après leur déploiement, comme défini par l'exigence 6.6 des normes PCI DSS.</i></p>	<p>Les vulnérabilités en matière de sécurité présentes dans le code personnalisé sont généralement exploitées par les individus malveillants pour accéder à un réseau et compromettre les données de titulaire de carte. Les utilisateurs qui maîtrisent les techniques de codage sécurisé devraient passer en revue le code afin d'en identifier les failles éventuelles.</p>

Exigence	Directive
<p>6.4 Suivre les procédures de contrôle des changements pour toutes les modifications apportées à des composants du système. Les procédures doivent inclure ce qui suit :</p>	<p>En l'absence de contrôles appropriés des modifications apportées aux logiciels, les fonctions de sécurité peuvent être omises ou rendues inopérantes par accident ou délibérément, des irrégularités peuvent se produire lors du traitement ou du code malicieux peut être introduit. Si les politiques régissant le contrôle des renseignements relatifs aux employés et les contrôles d'accès au système ne sont pas adéquates, il y a un risque que des intrus et des utilisateurs non formés aient un accès illimité au code logiciel, que des employés qui ne travaillent plus pour la société aient accès aux systèmes pour les endommager et que des actions non autorisées ne soient pas détectées.</p>
<p>6.4.1 Documentation de l'impact</p>	<p>L'impact de la modification doit être décrit de sorte que toutes les parties concernées puissent s'organiser de manière appropriée pour gérer tout changement du traitement.</p>
<p>6.4.2 Validation de la gestion par les parties appropriées</p>	<p>L'approbation des responsables indique que la modification est légitime et autorisée par l'entreprise.</p>
<p>6.4.3 Tests de fonctionnalité opérationnelle</p>	<p>Des tests approfondis doivent être effectués pour vérifier que toutes les actions sont prévues, que toutes les conditions d'erreur possibles réagissent de manière appropriée, etc.</p>
<p>6.4.4 Procédures de suppression</p>	<p>Chaque modification doit être associée à des procédures de suppression en cas d'échec afin de pouvoir établir l'état antérieur.</p>
<p>6.5 Développer toutes les applications Web (internes et externes, y compris l'accès administratif Web au produit) sur la base des meilleures pratiques de codage sécurisé, telles que celles décrites dans le Guide de l'OWASP (<i>Open Web Application Security Project</i>). Prévenir les vulnérabilités de codage courantes dans les processus de développement de logiciel, afin d'inclure les éléments suivants :</p> <p><i>Remarque : Les vulnérabilités décrites aux points 6.5.1 à 6.5.10 étaient actualisées dans le guide de l'OWASP au moment de la publication des normes PCI DSS v1.2. Toutefois, si le guide de l'OWASP est mis à jour, il convient d'utiliser la version la plus récente de ces exigences.</i></p>	<p>La couche Application implique des risques élevés et peut être la cible de menaces tant internes qu'externes. En l'absence de mesures de sécurité adéquates, les données de titulaire de carte et autres informations confidentielles de la société peuvent être exposées à ces risques, ce qui peut nuire à l'entreprise et à sa réputation, ainsi qu'à ses clients.</p>

Exigence	Directive
<p>6.5.1 Attaques XSS (Cross-Site Scripting)</p>	<p>Tous les paramètres doivent être validés avant leur inclusion. Des attaques XSS se produisent chaque fois qu'une application extrait les données fournies par un utilisateur et les transmet à un navigateur Web sans les valider ou les encoder au préalable. XSS permet aux pirates d'exécuter un script dans le navigateur de la victime, qui peut détourner des sessions utilisateur, usurper des sites Web, introduire éventuellement des vers, etc.</p>
<p>6.5.2 Attaques par injection, notamment les injections de commandes SQL. Considérer également les attaques par injection LDAP et Xpath ainsi que les autres attaques par injection.</p>	<p>Validez les données entrées pour vérifier que les données utilisateur ne peuvent pas modifier le sens des commandes et des requêtes. Les attaques par injection, en particulier par injection SQL, sont courantes dans les applications Web. Une attaque par injection se produit lorsque les données saisies par un utilisateur sont transmises à un programme d'interprétation dans le cadre d'une commande ou d'une requête. Les données hostiles du pirate trompe le programme d'interprétation et le pousse à exécuter des commandes indésirables ou à modifier les données, permettant alors au pirate d'attaquer des composants du réseau par le biais de l'application, de lancer des attaques telles que la saturation de la mémoire tampon, ou de révéler des informations confidentielles ainsi que la fonctionnalité de l'application serveur. Cette méthode est également courante pour réaliser des transactions frauduleuses sur les sites Web de e-commerce. Les informations contenues dans les requêtes Web doivent être validées avant d'être transmises à l'application Web, par exemple en vérifiant tous les caractères alphabétiques, le mélange de caractères alphanumériques, etc.</p>
<p>6.5.3 Exécution de fichiers malveillants</p>	<p>Validez les données entrées pour vérifier que l'application n'accepte pas les noms de fichiers ou les fichiers d'utilisateurs inattendus. Le code vulnérable à RFI (Remote File Inclusion) permet aux pirates d'inclure des données et du code hostiles, entraînant alors des attaques dévastatrices, par exemple l'endommagement de l'intégralité d'un serveur. Les attaques reposant sur l'exécution de fichiers malicieux affectent le code PHP et XML ainsi que tout environnement qui accepte les noms de fichiers ou les fichiers d'utilisateurs.</p>
<p>6.5.4 Références d'objets directes non sécurisées</p>	<p>N'exposez en aucun cas les références à des objets internes aux utilisateurs. Une référence d'objet directe existe lorsqu'un développeur expose la référence à un objet d'implémentation interne, telle qu'un fichier, un répertoire, un enregistrement de base de données ou une clé, par exemple une adresse URL ou un paramètre de formulaire. Les pirates peuvent manipuler ces références pour accéder à d'autres objets sans y être autorisés.</p>

Exigence	Directive
<p>6.5.5 Attaques CSRF (Cross-Site Request Forgery)</p>	<p>Ne répondez pas aux informations d'autorisation ni aux jetons automatiquement envoyés par les navigateurs. Une attaque CSRF force le navigateur d'une victime connectée à envoyer une requête pré-authentifiée à une application Web vulnérable, qui force à son tour le navigateur en question à exécuter une action hostile au bénéfice du pirate. Les attaques CSRF peuvent être aussi puissantes que l'application Web attaquée.</p>
<p>6.5.6 Fuites d'information et traitement inapproprié des erreurs</p>	<p>Ne laissez filtrer aucune information par le biais de messages d'erreur ni par aucun autre moyen. Les applications peuvent accidentellement laisser filtrer des informations sur leur configuration ou les mécanismes internes, ou elles peuvent contrevenir aux politiques de confidentialité par le biais de divers problèmes liés aux applications. Les pirates exploitent cette faiblesse pour subtiliser des données sensibles ou lancer des attaques plus importantes. En outre, la gestion incorrecte des erreurs fournit des informations susceptibles d'aider un individu malveillant à endommager le système. Si un individu malveillant est en mesure de créer des erreurs que l'application Web ne gère pas correctement, il peut alors accéder à des informations détaillées concernant le système, créer des interruptions par déni de service, entraîner l'échec de la sécurité ou provoquer l'arrêt du serveur. Par exemple, le message indiquant que le « mot de passe saisi est incorrect » l'informe que le nom d'utilisateur entré est correct et qu'il devrait se concentrer uniquement sur le décryptage du mot de passe. Utilisez des messages d'erreur plus génériques, comme « Impossible de vérifier les données ».</p>
<p>6.5.7 Rupture dans la gestion des authentifications et des sessions</p>	<p>Authentifiez les utilisateurs de manière appropriée et protégez correctement les informations de compte et les jetons de session. Il arrive souvent que les informations de compte et les jetons de session ne soient pas correctement protégés. Les pirates compromettent les mots de passe, les clés ou les jetons d'authentification pour usurper l'identité d'autres utilisateurs.</p>
<p>6.5.8 Stockage cryptographique non sécurisé</p>	<p>Empêchez les attaques cryptographiques. Les applications Web utilisent rarement les fonctions cryptographiques de manière adéquate pour protéger les données et les informations d'identification. Les pirates exploitent les données mal protégées pour usurper des identités et commettre d'autres délits, telles que des fraudes à la carte bancaire.</p>
<p>6.5.9 Communications non sécurisées</p>	<p>Cryptez correctement toutes les communications authentifiées et sensibles. Il arrive fréquemment que les applications ne cryptent pas le trafic réseau lorsqu'il convient de protéger des communications sensibles.</p>

Exigence	Directive
<p>6.5.10 Impossibilité de limiter l'accès aux URL</p>	<p>Appliquez le contrôle des accès de façon cohérente au niveau de la couche Présentation et de la logique applicative pour toutes les URL. Il arrive fréquemment qu'une application ne protège la fonctionnalité sensible qu'en empêchant l'affichage des liens ou des adresses URL aux utilisateurs non autorisés. Les pirates peuvent exploiter cette faiblesse pour accéder aux données et exécuter des opérations non autorisées en accédant directement à ces URL.</p>
<p>6.6 Pour les applications Web orientées public, traiter les nouvelles menaces et vulnérabilités de manière régulière et veiller à ce que ces applications soient protégées contre les attaques connues à l'aide de l'une des méthodes suivantes :</p> <ul style="list-style-type: none"> ▪ Examen des applications Web orientées public à l'aide d'outils ou de méthodes d'évaluation de la sécurité et de la vulnérabilité des applications automatiques ou manuels, au moins une fois par an et après toute modification ▪ Installation d'un pare-feu pour applications Web devant les applications Web orientées public 	<p>Les attaques sur les applications orientées vers le Web sont courantes, sont souvent couronnées de succès et résultent de pratiques déficientes en matière de codage. Cette exigence d'examen des applications ou d'installations de pare-feu pour les applications Web vise à réduire considérablement les risques auxquels sont exposées les applications Web orientées public qui entraînent l'accès d'intrus aux données de titulaire de carte.</p> <ul style="list-style-type: none"> ▪ Des outils ou des méthodes d'évaluation de la sécurité et de la vulnérabilité automatiques ou manuels qui passent en revue et/ou analysent les vulnérabilités des applications peuvent être utilisés pour satisfaire cette exigence ▪ Les pare-feu pour applications Web filtrent et bloquent le trafic non essentiel au niveau de la couche Application. Utilisé conjointement avec un pare-feu réseau, un pare-feu pour applications Web correctement configuré empêche les attaques au niveau de la couche Application si les applications sont incorrectement configurées ou codées. <p>Voir <i>Complément d'informations : Exigence 6.6 clarifiant les révisions d'applications et les pare-feu d'applications Web</i> (www.pcisecuritystandards.org) pour plus d'informations.</p>

Directives relatives aux exigences 7, 8 et 9 : Mise en œuvre de mesures de contrôle d'accès strictes

Exigence 7 : Restreindre l'accès aux données de titulaire de carte aux seuls individus qui doivent les connaître

Pour veiller à ce que les données stratégiques ne soient accessibles qu'au personnel autorisé, des systèmes et des processus doivent être mis en place pour restreindre l'accès à ces données aux seuls individus qui doivent les connaître et en fonction de leurs responsabilités professionnelles. En d'autres termes, les droits d'accès ne sont accordés qu'au plus petit nombre de données nécessaires et en fonction des tâches à effectuer.

Exigence	Directive
<p>7.1 Restreindre l'accès aux composants du système et aux données de titulaire de carte aux seuls individus qui doivent y accéder pour mener à bien leur travail. Les restrictions d'accès doivent inclure ce qui suit :</p> <p>7.1.1 Restriction des droits d'accès accordés aux ID d'utilisateur privilégiés en octroyant les privilèges les plus faibles qui sont nécessaires pour la réalisation du travail</p> <p>7.1.2 L'octroi des privilèges se fait sur la base de la classification et de la fonction professionnelles de chaque employé</p> <p>7.1.3 Nécessité de faire signer par les responsables un formulaire d'autorisation qui précise les privilèges requis</p> <p>7.1.4 Mise en œuvre d'un système de contrôle d'accès automatique</p>	<p>Plus le nombre de personnes ayant accès aux données de titulaire de carte est élevé, plus il y a de risques que le compte d'un utilisateur soit utilisé de manière frauduleuse. Restreindre l'accès aux seuls individus qui doivent y accéder pour mener à bien leur travail aidera votre entreprise à éviter la manipulation des données de titulaire de carte par des utilisateurs inexpérimentés ou malveillants. L'octroi de droits d'accès portant sur la plus petite quantité de données nécessaires et au niveau le plus faible requis pour la réalisation du travail est désigné par le terme « principe du besoin de connaître ». L'octroi de privilèges sur la base de la classification et de la fonction professionnelles des individus est appelé « contrôle d'accès en fonction du rôle » (ou RBAC, Role-Based Access Control). Votre entreprise devrait mettre en place une politique et des processus clairement définis pour le contrôle d'accès aux données en fonction du « principe du besoin de connaître » et du « contrôle d'accès en fonction du rôle », afin de définir comment et à qui accorder l'accès.</p>

Exigence	Directive
<p>7.2 Définir un mécanisme pour les composants de systèmes comptant plusieurs utilisateurs, qui limite l'accès aux seuls utilisateurs qui doivent accéder aux données et qui est configuré pour « refuser tous les accès » à moins qu'ils ne soient explicitement autorisés. Ce système de contrôle d'accès doit inclure les éléments suivants :</p> <p><i>Remarque : En d'autres termes, les droits d'accès ne sont accordés qu'au plus petit nombre de données nécessaires et en fonction des tâches à effectuer.</i></p> <p>7.2.1 Couverture de tous les composants du système</p> <p>7.2.2 L'octroi de privilèges aux individus repose sur leur classification et leur fonction professionnelles</p> <p>7.2.3 Configuration par défaut du paramètre « Refuser tout »</p>	<p>En l'absence d'un mécanisme de restriction de l'accès en fonction du besoin de connaître les informations, un utilisateur peut, à son insu, se voir accorder l'accès aux données de titulaire de carte. L'usage d'un système ou d'un mécanisme de contrôle d'accès automatisé est essentiel pour gérer plusieurs utilisateurs. Ce système doit être défini conformément à la politique et aux processus de contrôle d'accès de votre entreprise (notamment « principe du besoin de connaître » et « contrôle d'accès en fonction du rôle »), doit gérer l'accès à tous les composants du système et doit intégrer un paramètre par défaut « Refuser tout » pour veiller à ce que personne ne se voit accorder l'accès tant qu'une règle octroyant spécifiquement cet accès n'a pas été définie.</p>

Exigence 8 : Affecter un ID unique à chaque utilisateur d'ordinateur

En affectant un identifiant (ID) unique à chaque utilisateur, on s'assure que chacun sera personnellement responsable de ses actes. Les actions sur des données et des systèmes stratégiques peuvent alors être exécutées par des utilisateurs clairement identifiés et habilités à le faire.

Exigence	Directive
<p>8.1 Affecter à tous les utilisateurs un ID unique avant de les autoriser à accéder à des composants du système ou aux données de titulaire de carte.</p>	<p>En veillant à ce que chaque utilisateur soit identifié de manière unique, au lieu d'utiliser un ID unique pour plusieurs employés, l'entreprise peut maintenir la responsabilité de chaque individu pour ses actions et un journal d'audit efficace par employé. Cela contribuera à accélérer la résolution des problèmes et à en limiter les conséquences en cas d'erreur de manipulation ou d'utilisation à des fins malveillantes.</p>
<p>8.2 Outre l'affectation d'un ID unique, employer au moins l'une des méthodes suivantes pour authentifier tous les utilisateurs :</p> <ul style="list-style-type: none"> ▪ Mot de passe ▪ Authentification à deux facteurs (par exemple, dispositifs à jetons, cartes à puce, biométrie ou clés publiques) 	<p>Ces éléments d'authentification, lorsqu'ils sont utilisés en plus des ID uniques, contribuent à protéger les ID uniques des utilisateurs contre les risques de divulgation (puisque le pirate doit connaître l'ID unique et le mot de passe ou tout autre élément d'authentification).</p>
<p>8.3 Intégrer l'authentification à deux facteurs pour l'accès à distance (accès au niveau du réseau depuis l'extérieur du réseau) des employés, des administrateurs et de tiers au réseau. Utiliser des technologies telles que RADIUS (Remote Authentication and Dial-in Service), TACACS (Terminal Access Controller Un système de contrôle d'accès) avec des jetons ou VPN (basé sur SSL/TLS ou IPSEC) avec des certificats individuels.</p>	<p>L'authentification à deux facteurs requiert deux formes d'authentification pour les accès à hauts risques, tels que ceux émanant de l'extérieur de votre réseau. Pour renforcer sa sécurité, votre entreprise peut également envisager le recours à l'authentification à deux facteurs lors de l'accès à des réseaux impliquant un niveau de sécurité supérieure à partir de réseaux d'un niveau de sécurité inférieur, par exemple l'accès aux serveurs de production/bases de données contenant les données de titulaire de carte (niveau de sécurité élevé) à partir d'ordinateurs de bureau de l'entreprise (niveau de sécurité inférieur).</p>
<p>8.4 Rendre tous les mots de passe illisibles pendant la transmission et le stockage sur tous les composants du système à l'aide d'une méthode de cryptographie robuste (définie dans le <i>Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS</i>).</p>	<p>De nombreux équipements et applications réseau transmettent l'ID utilisateur et le mot de passe non crypté sur le réseau et/ou stockent également les mots de passes sans cryptage. Un individu malveillant peut facilement intercepter l'ID utilisateur et le mot de passe non cryptés ou lisibles pendant leur transmission à l'aide d'un « renifleur », ou il peut directement accéder aux ID utilisateur et aux mots de passe non cryptés dans les fichiers où ils sont stockés et utiliser ces données subtilisées pour accéder illicitement au réseau.</p>

Exigence	Directive
<p>8.5 S'assurer qu'une gestion appropriée des mots de passe et de l'authentification des utilisateurs est mise en œuvre pour les utilisateurs non-consommateurs et les administrateurs sur tous les composants du système comme suit :</p>	<p>Étant donné que l'une des premières étapes qu'un individu malveillant suivra pour compromettre un système consiste à exploiter la faiblesse ou la non-existence de mots de passe, il est important de mettre en place les processus appropriés pour l'authentification des utilisateurs et la gestion des mots de passe.</p>
<p>8.5.1 Contrôler l'ajout, la suppression et la modification d'ID d'utilisateur, d'informations d'identification et d'autres objets identifiant.</p>	<p>Pour s'assurer que les utilisateurs ajoutés sur vos systèmes sont tous valides et reconnus, l'ajout, la suppression et la modification d'ID utilisateurs doivent toujours être gérés et contrôlés par un groupe restreint possédant une autorité spécifique. La gestion de ces ID utilisateur doit être limitée à ce petit groupe.</p>
<p>8.5.2 Vérifier l'identité des utilisateurs avant de réinitialiser leur mot de passe.</p>	<p>De nombreux individus malveillants ont recours à « l'ingénierie sociale », par exemple, en appelant un service d'assistance et en se faisant passer pour un utilisateur légitime, pour obtenir la modification du mot de passe afin de pouvoir utiliser un ID utilisateur. Envisagez l'utilisation d'une « question secrète » à laquelle seul l'utilisateur véritable peut répondre pour aider les administrateurs à l'identifier avant d'accepter de redéfinir ses mots de passe. Veillez à ce que ces questions soient correctement protégées et qu'elles ne soient divulguées à personne.</p>
<p>8.5.3 Définir des mots de passe initiaux uniques pour chaque utilisateur et les modifier immédiatement après la première utilisation.</p>	<p>Si le même mot de passe est utilisé pour chaque nouvel utilisateur configuré, un utilisateur interne, un ancien employé ou un individu malveillant peut connaître ou facilement découvrir ce mot de passe et l'utiliser pour accéder aux comptes.</p>
<p>8.5.4 Révoquer immédiatement l'accès de tout utilisateur qui ne travaille plus pour la société.</p>	<p>Si les employés qui ont quitté la société ont toujours accès au réseau par le biais de leurs comptes d'utilisateur, ils pourront accéder aux données de titulaire de carte alors qu'ils n'en ont plus besoin, voire aux fins de nuire. Un utilisateur malveillant peut également exploiter les anciens comptes et/ou les comptes inutilisés. Envisagez de mettre en place, en concertation avec le service des ressources humaines, un processus de notification de tout employé qui quitte la société afin que son compte d'utilisateur soit rapidement désactivé.</p>
<p>8.5.5 Supprimer/désactiver les comptes d'utilisateur inactifs au moins tous les 90 jours.</p>	<p>L'existence de comptes inactifs permet à un utilisateur non autorisé d'exploiter les comptes non utilisés pour accéder aux données de titulaire de carte.</p>

Exigence	Directive
<p>8.5.6 Activer les comptes utilisés par les fournisseurs pour la maintenance à distance pendant la période nécessaire seulement.</p>	<p>En autorisant les fournisseurs (par ex. les fournisseurs de points de vente) à accéder à votre réseau 24 heures sur 24 et 7 jours sur 7 au cas où ils auraient besoin d'intervenir sur vos systèmes, vous augmentez les risques d'accès non autorisés, qu'il s'agisse d'un utilisateur appartenant à l'environnement du fournisseur ou d'un individu malveillant qui découvre et exploite ce point d'entrée dans votre réseau en permanence disponible. Reportez-vous également aux points 12.3.8 et 12.3.9 pour plus d'informations à ce sujet.</p>
<p>8.5.7 Communiquer les politiques et les procédures relatives aux mots de passe à tous les utilisateurs qui ont accès aux données de titulaire de carte.</p>	<p>Communiquer les procédures relatives aux mots de passe à tous les utilisateurs aide ces derniers à comprendre et à respecter les politiques en question, et à rester vigilants face à tout individu malveillant qui pourrait tenter d'exploiter leurs mots de passe pour accéder aux données de titulaire de carte (par exemple, en appelant un employé pour lui demander son mot de passe en vue de « résoudre un problème »).</p>
<p>8.5.8 Ne pas utiliser des comptes et des mots de passe collectifs, partagés ou génériques.</p>	<p>Si plusieurs utilisateurs partagent les mêmes compte et mot de passe, il est alors impossible de déterminer leurs responsabilités ni de consigner efficacement leurs actions individuelles, puisque celles-ci peuvent avoir été exécutées par n'importe quel membre du groupe.</p>
<p>8.5.9 Modifier les mots de passe utilisateur au moins tous les 90 jours.</p>	<p>Des mots de passe complexes sont la première ligne de défense sur un réseau, puisqu'un individu malveillant commencera souvent par rechercher les comptes dont les mots de passe sont faibles ou non existants. Si les mots de passe sont courts, faciles à deviner ou valides pendant une période prolongée sans être modifiés, un individu malveillant n'aura pas trop de mal à les découvrir et à s'introduire sur un réseau sous l'identité d'un ID utilisateur valide. Des mots de passe complexes peuvent être définis et gérés conformément à ces exigences en activant les fonctions de sécurité des mots de passe et des comptes intégrées à votre système d'exploitation (par exemple, Windows), à vos réseaux, à vos bases de données et autres plates-formes.</p>
<p>8.5.10 Exiger des mots de passe comportant au moins sept caractères.</p>	
<p>8.5.11 Définir des mots de passe comportant des caractères alphanumériques.</p>	
<p>8.5.12 Interdire à un utilisateur de soumettre un nouveau mot de passe identique à l'un de ses quatre derniers mots de passe.</p>	
<p>8.5.13 Limiter les tentatives d'accès répétées en verrouillant l'ID d'utilisateur après six tentatives au maximum.</p>	<p>En l'absence de mécanismes de verrouillage de compte, un pirate pourra en permanence essayer de deviner un mot de passe à l'aide d'outils manuels ou automatiques (par exemple, craquage de mots de passe), jusqu'à parvenir à ses fins et accéder au compte d'un utilisateur.</p>

Exigence	Directive
<p>8.5.14 Régler la durée de verrouillage sur 30 minutes au moins ou jusqu'à ce que l'administrateur active l'ID d'utilisateur.</p>	<p>Si un compte est verrouillé car quelqu'un a essayé à plusieurs reprises d'en deviner le mot de passe, des contrôles retardant la réactivation de ce compte empêchent l'individu malveillant de poursuivre (il devra s'arrêter pendant au moins 30 minutes jusqu'à la réactivation du compte). Par ailleurs, si la réactivation doit être demandée, l'administrateur ou le service d'assistance peut valider que le titulaire du compte est à l'origine du verrouillage (par exemple, en raison d'une erreur de saisie).</p>
<p>8.5.15 Si une session reste inactive pendant plus de 15 minutes, demander à l'utilisateur de saisir de nouveau son mot de passe pour réactiver le terminal.</p>	<p>Lorsque les utilisateurs dont l'ordinateur a accès aux données de titulaire de carte ou au réseau critique s'éloignent de leur poste allumé, d'autres utilisateurs peuvent profiter de leur absence pour accéder illicitement à un compte et/ou le manipuler à des fins frauduleuses.</p>
<p>8.5.16 Authentifier tous les accès aux bases de données contenant des données de titulaire de carte. Cette exigence concerne les accès des applications, des administrateurs et de tous les autres utilisateurs.</p>	<p>Sans l'authentification de l'accès des utilisateurs aux bases de données et aux applications, les risques d'accès non autorisés ou à des fins malveillantes augmentent et ceux-ci ne peuvent pas être consignés dans les journaux puisque les utilisateurs en question ne sont pas authentifiés et, par conséquent, sont inconnus du système. En outre, l'accès aux bases de données doit être accordé par programme seulement (par exemple, par le biais de procédures stockées), au non via un accès direct à la base de données par les utilisateurs finaux (à l'exception des administrateurs de base de données, qui ont un accès direct à la base de données pour mener à bien leurs obligations administratives).</p>

Exigence 9 : Restreindre l'accès physique aux données de titulaire de carte

Dans la mesure où tout accès physique à des données ou à des systèmes hébergeant des données de titulaire de carte permet à des individus d'accéder à des périphériques ou à des informations, et de supprimer des systèmes ou des copies papier, cet accès doit être restreint de façon appropriée.

Exigence	Directive
<p>9.1 Utiliser des contrôles d'accès aux installations appropriés pour restreindre et surveiller l'accès physique aux systèmes installés dans l'environnement des données de titulaire de carte.</p>	<p>En l'absence de contrôles d'accès physiques, des personnes non autorisées peuvent accéder aux locaux et aux informations sensibles, et peuvent modifier les configurations des systèmes, introduire des vulnérabilités dans le réseau, ou détruire ou subtiliser des équipements.</p>
<p>9.1.1 Installer des caméras vidéo ou d'autres mécanismes de contrôle d'accès pour surveiller l'accès des individus aux zones sensibles. Examiner les données enregistrées et les mettre en corrélation avec d'autres informations. Les conserver pendant trois mois au minimum, sauf stipulation contraire de la loi.</p> <p><i>Remarque : Par « zones sensibles », nous entendons tout centre de données, salle de serveurs ou zone abritant des systèmes qui stockent des données de titulaire de carte. Cette définition exclut les zones où ne sont installés que des terminaux de point de vente, tels que les zones de caisse dans un magasin.</i></p>	<p>Lors d'investigations sur les violations physiques, ces contrôles peuvent faciliter l'identification des individus qui accèdent physiquement aux zones stockant les données de titulaire de carte.</p>
<p>9.1.2 Restreindre l'accès physique aux prises réseau accessibles au public.</p>	<p>La restriction de l'accès aux prises réseau empêchera les individus malveillants de brancher leur ordinateur aux prises réseau disponibles qui leur donneraient accès aux ressources sur les réseaux internes. Envisagez de désactiver les prises réseau lorsqu'elles ne sont pas utilisées et de ne les réactiver que lorsque vous en avez besoin. Dans les espaces publics, tels que les salles de conférence, mettez en place des réseaux privés afin de permettre aux fournisseurs et aux visiteurs d'accéder à Internet seulement, sans pouvoir accéder à votre réseau interne.</p>

Exigence	Directive
<p>9.1.3 Restreindre l'accès physique aux passerelles, appareils mobiles de poche et points d'accès sans fil.</p>	<p>En l'absence de mécanismes de sécurité sur les composants et les équipements sans fil, les utilisateurs malveillants pourraient exploiter les équipements sans fil de votre entreprise laissés sans surveillance pour accéder à vos ressources réseau et même connecter leurs propres équipements à votre réseau sans fil, leur octroyant ainsi un accès non autorisé. Envisagez la mise en place de passerelles et de points d'accès sans fil dans les zones de stockage sécurisées, par exemple des salles de serveurs ou des armoires fermées à clé. Assurez-vous qu'un cryptage robuste est activé. Activez le verrouillage automatique des équipements portables sans fil lorsqu'ils restent inactifs pendant une période prolongée et configurez vos équipements pour exiger la saisie d'un mot de passe au démarrage.</p>
<p>9.2 Élaborer des procédures qui aident l'ensemble du personnel à faire facilement la distinction entre les employés et les visiteurs, en particulier dans les zones où sont accessibles les données de titulaire de carte.</p> <p><i>Dans le cadre de cette exigence, le terme « employé » désigne les employés à temps plein et à temps partiel, les intérimaires ainsi que les sous-traitants et les consultants qui « résident » sur le site de l'entité. Un « visiteur » est défini comme un fournisseur, l'invité d'un employé, le personnel de service ou tout individu présent au sein des locaux pendant une période courte, n'excédant généralement pas une journée.</i></p>	<p>En l'absence de systèmes de badge et de contrôles aux portes, des utilisateurs non autorisés et malveillants peuvent facilement accéder à vos installations pour subtiliser, désactiver, mettre à mal ou détruire vos systèmes stratégiques et les données de titulaire de carte. Pour un contrôle optimal, envisagez la mise en place d'un système d'accès protégé par badge ou carte à l'entrée et à la sortie des zones de travail impliquant les données de titulaire de carte.</p>
<p>9.3 S'assurer que tous les visiteurs sont traités de la manière suivante :</p>	<p>Le contrôle des visiteurs est essentiel pour réduire les risques que des personnes non autorisées ou malveillantes accèdent à vos installations, et éventuellement aux données de titulaire de carte.</p>

Exigence	Directive
<p>9.3.1 Une autorisation d'accès leur est donnée avant de pénétrer dans les zones où sont traitées et conservées les données de titulaire de carte.</p> <p>9.3.2 Ils reçoivent un jeton physique (par exemple, badge ou dispositif d'accès) doté d'une date d'expiration et qui identifie bien les visiteurs comme ne faisant pas partie du personnel.</p> <p>9.3.3 Il leur est demandé de rendre le jeton physique avant de quitter les locaux ou à la date d'expiration.</p>	<p>Le contrôle des visiteurs est essentiel pour veiller à ce que ceux-ci ne puissent pénétrer que dans les zones autorisées, qu'ils soient identifiables en tant que visiteurs de sorte que les employés puissent surveiller leurs activités et que leur accès ne soit pas valide au-delà de la durée de leur visite légitime.</p>
<p>9.4 Utiliser un registre des visites pour tenir un contrôle physique de la circulation des visiteurs. Y indiquer le nom du visiteur, l'entreprise qu'il représente et l'employé qui autorise son accès physique. Conserver ce registre pendant trois mois au minimum, sauf stipulation contraire de la loi.</p>	<p>Un journal des visiteurs indiquant un minimum d'informations concernant les visiteurs est facile et peu coûteux à tenir et vous aidera, en cas de violation de la sécurité des données, à identifier les accès physiques à un bâtiment ou une salle et les accès potentiels aux données de titulaire de carte. Envisagez la mise en place de registres à l'entrée des locaux, en particulier dans les zones où sont présentes les données de titulaire de carte.</p>
<p>9.5 Ranger les sauvegardes sur support en lieu sûr, de préférence hors de l'installation, par exemple sur un autre site ou un site de secours, ou encore un site de stockage commercial. Inspecter la sécurité du site au moins une fois par an.</p>	<p>Si elles sont stockées dans un local non sécurisé, les sauvegardes contenant les données de titulaire de carte peuvent être facilement perdues, volées ou copiées à des fins malveillantes. Pour en sécuriser le stockage, envisagez de faire appel aux services d'une entreprise de stockage de données commerciales OU, dans le cas d'une petite entité, envisagez la location d'un coffre-fort auprès d'une banque.</p>
<p>9.6 Ranger physiquement en lieu sûr tous les documents papier et les supports électroniques contenant les données de titulaire de carte.</p>	<p>Lorsqu'elles se trouvent sur un support portable, lorsqu'elles sont imprimées ou lorsqu'elles sont laissées sur le bureau d'un employé, les données de titulaire de carte sont susceptibles d'être consultées, copiées ou scannées sans autorisation. Envisagez la mise en place de procédures et de processus de protection de ces données sur les supports diffusés à des utilisateurs internes et/ou externes. En l'absence de telles procédures, vous exposez ces données à des risques de perte, de vol ou d'utilisation frauduleuse.</p>

Exigence	Directive
9.7 Assurer un contrôle strict de la distribution interne ou externe de tout type de support contenant des données de titulaire de carte, notamment ce qui suit :	
9.7.1 Classifier les supports de manière à les identifier comme contenant des informations confidentielles.	Il est possible que les supports qui ne sont pas identifiés comme étant confidentiels ne soient pas traités avec le soin nécessaire et qu'ils soient perdus ou volés. Incluez un processus de classification des supports aux procédures recommandées dans l'exigence 9.6 ci-dessus.
9.7.2 Envoyer les supports par coursier ou toute autre méthode d'expédition qui peut faire l'objet d'un suivi.	S'ils sont envoyés sans suivi, par exemple par courrier postal normal, les supports risquent d'être perdus ou volés. Faites appel aux services d'un coursier de confiance pour l'envoi de tout support contenant les données de titulaire de carte, de manière à pouvoir localiser le colis à tout moment à l'aide de son système de suivi.
9.8 S'assurer que les responsables approuvent tous les supports contenant des données de titulaire de carte déplacées d'une zone sécurisée (en particulier s'ils sont distribués par des personnes).	En l'absence d'un processus approuvé par les responsables, les données de titulaire de carte qui quittent une zone sécurisée peuvent être perdues ou subtilisées. Sans un processus strict, il n'est pas possible de localiser à tout moment l'emplacement des supports, ni de savoir comment elles sont protégées. Incluez le développement d'un processus approuvé par les responsables pour le déplacement des supports dans les procédures recommandées à l'exigence 9.6 ci-dessus.
9.9 Assurer un contrôle strict du stockage et de l'accessibilité des supports contenant des données de titulaire de carte.	En l'absence de méthodes d'inventaire et de contrôles du stockage stricts, les supports volés ou manquants pourraient passer inaperçus pendant une période indéterminée. Incluez le développement d'un processus limitant l'accès aux supports contenant les données de titulaire de carte dans les procédures recommandées par l'exigence 9.6 ci-dessus.
9.9.1 Tenir de manière appropriée les journaux d'inventaire de tous les supports et effectuer un inventaire des supports au moins une fois par an.	Si les supports ne font pas l'objet d'un inventaire, ceux qui ont été volés ou perdus pourraient passer inaperçus pendant une période indéterminée. Incluez le développement d'un processus d'inventaire et de stockage sécurisé des supports dans les procédures recommandées par l'exigence 9.6 ci-dessus.

Exigence	Directive
<p>9.10 Détruire les supports contenant des données de titulaire de carte lorsqu'ils ne sont plus nécessaires à des fins commerciales ou juridiques comme suit :</p>	<p>Si aucune mesure n'est prise pour la destruction des informations contenues sur les disques durs d'ordinateurs, sur CD et sur papier, ces données peuvent être exposées à des risques lors de leur élimination, et occasionner alors des pertes financières ou nuire à votre réputation. Par exemple, des individus malveillants peuvent employer une technique appelée « dumpster diving », qui consiste à fouiller les poubelles et les corbeilles, afin d'y rechercher des informations utiles pour lancer une attaque. Incluez le développement d'un processus de destruction approprié des supports contenant les données de titulaire de carte, notamment le stockage approprié de ces supports avant leur destruction, dans les procédures recommandées par l'exigence 9.6 ci-dessus.</p>
<p>9.10.1 Déchiqueter, brûler ou réduire en pâte les documents papier de sorte que les données de titulaire de carte ne puissent pas être reconstituées.</p>	
<p>9.10.2 Rendre les données de titulaire de carte sur support électronique irrécupérables de sorte que les informations ne puissent pas être reconstituées.</p>	

Directives relatives aux exigences 10 et 11 : Surveillance et test réguliers des réseaux

Exigence 10 : Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données de titulaire de carte

Les mécanismes de journalisation et la possibilité de suivre les activités des utilisateurs sont essentiels pour prévenir, détecter ou minimiser l'impact d'une altération des données. La présence de journaux dans tous les environnements permet de suivre de près, d'émettre des alertes et d'analyser les incidents éventuels. En l'absence de journaux retraçant les activités du système, il est très difficile de déterminer la cause d'une anomalie.

Exigence	Directive
<p>10.1 Définir un processus pour associer chaque accès aux composants du système (en particulier les accès avec des droits administrateur, tels que root) à un utilisateur individuel.</p>	<p>Il est essentiel de disposer d'un processus ou d'un système qui établisse un lien entre l'accès des utilisateurs et les composants du système auxquels ils ont accédé, en particulier pour les utilisateurs disposant de privilèges d'administration. Ce système génère les journaux d'audit et permet de retracer les activités suspectes d'un utilisateur particulier. Les équipes en charge des analyses après incident s'appuient principalement sur ces journaux pour lancer leur enquête.</p>
<p>10.2 Mettre en œuvre des journaux d'audit automatiques pour tous les composants du système afin de reconstituer les événements suivants :</p> <ul style="list-style-type: none"> 10.2.1 Tous les accès d'utilisateurs individuels aux données de titulaire de carte 10.2.2 Toutes les actions exécutées par tout utilisateur avec des droits root ou administrateur 10.2.3 Accès à tous les journaux d'audit 10.2.4 Tentatives d'accès logique non valides 10.2.5 Utilisation des mécanismes d'identification et d'authentification 10.2.6 Initialisation des journaux d'audit 10.2.7 Création et suppression d'objets au niveau système 	<p>Les individus malveillants sur le réseau effectuent généralement plusieurs tentatives d'accès sur les systèmes ciblés. La création de journaux d'audit consignnant les activités suspectes alertent l'administrateur système, envoient des données à d'autres mécanismes de surveillance (tels des systèmes de détection d'intrusions) et fournissent un historique pour le suivi après incident.</p>

Exigence	Directive
<p>10.3 Consigner dans les journaux d'audit au moins les entrées suivantes pour chaque événement :</p> <ul style="list-style-type: none"> 10.3.1 Identification des utilisateurs 10.3.2 Type d'événement 10.3.3 Date et heure 10.3.4 Indication de succès ou d'échec 10.3.5 Origine de l'événement 10.3.6 Identité ou nom des données, du composant du système ou de la ressource affectés 	<p>La consignation de ces entrées pour les événements consignables au point 10.2 permet d'identifier rapidement les intrusions potentielles, avec suffisamment de détails pour en identifier l'auteur, l'objet, l'emplacement et la méthode employée.</p>
<p>10.4 Synchroniser toutes les heures et horloges système critiques.</p>	<p>Lorsqu'un individu malveillant pénètre sur le réseau, il tentera souvent de modifier l'horodatage de ses actions dans les journaux d'audit afin d'empêcher la détection de ses activités. Pour les équipes en charge des analyses après incident, l'heure de chaque activité est essentielle pour déterminer la manière dont les systèmes ont été compromis. Un individu malveillant peut également essayer de modifier directement l'horloge sur un serveur d'horloge, si les restrictions d'accès ne sont pas adéquates, afin de rétablir l'heure précédant son intrusion dans le réseau.</p>
<p>10.5 Protéger les journaux d'audit de sorte qu'ils ne puissent pas être modifiés.</p>	<p>Un individu malveillant qui pénètre dans le réseau essaiera souvent de modifier les journaux d'audit en vue de masquer son activité. En l'absence d'une protection adéquate des journaux d'audit, l'exhaustivité, l'exactitude et l'intégrité de ces derniers ne pourront pas être garanties et les journaux d'audit peuvent s'avérer inutiles en tant qu'outil d'investigation après l'endommagement du système.</p>

Exigence	Directive
<p>10.5.1 Limiter l'affichage des journaux d'audit aux utilisateurs qui en ont besoin pour mener à bien leur travail.</p> <p>10.5.2 Protéger les fichiers journaux d'audit contre toute modification non autorisée.</p> <p>10.5.3 Sauvegarder rapidement les fichiers journaux d'audit sur un serveur centralisé dédié à la journalisation ou sur des supports difficiles à altérer.</p> <p>10.5.4 Enregistrer les journaux des technologies orientées vers l'extérieur sur un serveur dédié à la journalisation sur le réseau local (LAN) interne.</p>	<p>La protection adéquate des journaux d'audit comprend un contrôle d'accès robuste (restriction stricte de l'accès aux journaux selon le « principe du besoin de connaître ») et l'utilisation d'un mécanisme d'isolation interne (de sorte que les journaux soient difficiles à trouver et à modifier). En enregistrant les journaux à partir de technologies orientées vers l'extérieur, telles que des pare-feu, des équipements sans fil, des serveurs DNS et des serveurs de messagerie, les risques de vol ou de modification de ces journaux sont réduits, puisqu'ils sont plus sécurisés sur le réseau interne.</p>
<p>10.5.5 Analyser les journaux à l'aide de logiciels de contrôle de l'intégrité des fichiers et de détection des modifications pour s'assurer que les données contenues dans les journaux ne peuvent pas être modifiées sans entraîner le déclenchement d'une alerte (alors que l'ajout de nouvelles données ne doit pas entraîner d'alerte).</p>	<p>Les systèmes de contrôle de l'intégrité des fichiers vérifient et signalent les modifications apportées aux fichiers stratégiques. Pour le contrôle de l'intégrité des fichiers, une entité vérifie généralement les fichiers qui ne sont pas régulièrement modifiés, mais dont la modification indique une intrusion possible. Dans le cas des fichiers journaux (qui ne changent pas fréquemment), les événements contrôlés sont, par exemple, leur suppression, une augmentation ou une réduction soudaine et importante de leur volume et toute autre indication qu'un individu malveillant les a altérés. Des outils prêts à l'emploi ainsi que des outils à code source libre sont disponibles pour le contrôle de l'intégrité des fichiers.</p>
<p>10.6 Passer en revue les journaux relatifs à tous les composants du système au moins une fois par jour. L'examen des journaux doit inclure les serveurs exécutant des fonctions de sécurité, tels que les serveurs IDS (système de détection d'intrusion) et AAA (Authentification, Authorisation et Accounting) (par exemple, RADIUS).</p> <p><i>Remarque : Les outils de journalisation, d'analyse et d'alerte peuvent être utilisés conformément à l'exigence 10.6.</i></p>	<p>De nombreuses violations se produisent pendant des jours ou des mois avant d'être détectées. La vérification quotidienne des journaux réduit la durée et l'exposition d'une violation potentielle. Le processus d'examen des journaux ne doit pas forcément être manuel. Les entités possédant un grand nombre de serveurs peuvent en particulier envisager l'utilisation d'outils de journalisation, d'analyse et d'alerte.</p>

Exigence	Directive
<p>10.7 Conserver l'historique des journaux d'audit pendant une année au moins, en gardant à portée de main les journaux des trois derniers mois au moins pour une analyse immédiate (par exemple, disponibles en ligne, dans des archives ou restaurables à partir d'une sauvegarde).</p>	<p>Les journaux doivent être conservés pendant une année au moins puisqu'il faut un certain temps avant d'observer une violation avérée et cela permet de donner aux enquêteurs suffisamment d'informations historiques pour déterminer la durée d'une violation potentielle et des systèmes éventuellement affectés. En gardant à portée de main les journaux des trois derniers mois, une entité peut rapidement identifier et minimiser l'impact d'un accès non autorisé aux données. Le stockage des bandes de sauvegarde hors site peut retarder la restauration des données, l'exécution d'analyses et l'identification des systèmes ou des données affectés.</p>

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

Des vulnérabilités sont sans cesse découvertes par des individus malveillants et des chercheurs, et sont introduites avec tout nouveau logiciel. Les composants du système, les processus et les logiciels personnalisés doivent être fréquemment testés afin de s'assurer que les contrôles de sécurité reflètent toujours les nouveaux environnements.

Exigence	Directive
<p>11.1 Tester la présence de points d'accès sans fil à l'aide d'un analyseur sans fil au moins une fois par trimestre ou en déployant un IDS/IPS sans fil pour identifier tous les périphériques sans fil qui sont utilisés.</p>	<p>L'implémentation et/ou l'exploitation de la technologie sans fil sur un réseau est l'un des chemins les plus fréquemment empruntés par les utilisateurs malveillants pour accéder au réseau et aux données de titulaire de carte. Si un périphérique ou un réseau sans fil est installé à l'insu d'une société, il peut permettre à un pirate de pénétrer sur le réseau facilement et à l'insu de tous. Outre les analyseurs sans fil, des scanneurs de ports et d'autres outils réseau détectant les périphériques sans fil peuvent être utilisés.</p> <p>Du fait de la facilité avec laquelle un point d'accès sans fil peut être connecté à un réseau, de la difficulté de détecter leur présence et du risque accru associé aux équipements sans fil non autorisés, ces analyses doivent être effectuées y compris s'il existe une politique interdisant l'usage de la technologie sans fil.</p> <p>Une entreprise devrait disposer, dans le cadre de son plan de réponse aux incidents, de procédures documentées à suivre en cas de détection d'un point d'accès sans fil non autorisé. Un système de détection et/ou de prévention d'intrusions (IDS/IPS) sans fil doit être configuré pour générer automatiquement une alerte, mais le plan doit également prévoir des procédures de réponse en cas de détection d'un équipement non autorisé lors d'une analyse manuelle.</p>

Exigence	Directive
<p>11.2 Analyser les vulnérabilités potentielles des réseaux internes et externes au moins une fois par trimestre et après tout changement significatif des réseaux (par exemple, l'installation de nouveaux composants du système, la modification de la topologie du réseau ou des règles des pare-feu, la mise à niveau de produits).</p> <p><i>Remarque : Des analyses des vulnérabilités externes doivent être effectuées une fois par trimestre par un prestataire de services d'analyse agréé par PCI SSC (Payment Card Industry Security Standards Council). Les analyses réalisées après la modification des réseaux peuvent être effectuées par le personnel interne de la société.</i></p>	<p>L'analyse des vulnérabilités est un outil automatisé exécuté sur les équipements et les serveurs réseau internes, en vue d'exposer les vulnérabilités potentielles et d'identifier les ports sur les réseaux qui pourraient être détectés et exploités par des individus malveillants. Une fois ces faiblesses identifiées, l'entité doit les corriger et réexécuter l'analyse afin de vérifier qu'elles ont bien été résolues.</p> <p>Lors de l'évaluation PCI DSS initiale de l'entreprise, il est possible que quatre analyses trimestrielles n'aient pas encore été exécutées. Si les résultats de l'analyse la plus récente sont satisfaisants et que des politiques et des procédures sont en place pour les futures analyses trimestrielles, l'objectif de cette exigence est satisfait. Dans ce cas, il n'est pas nécessaire de reporter une évaluation sur le terrain car les quatre analyses trimestrielles n'ont pas été effectuées.</p>
<p>11.3 Effectuer des tests de pénétration externe et interne au moins une fois par an et après tout changement ou mise à niveau significatif de l'infrastructure ou des applications (par exemple, mise à niveau du système d'exploitation ou ajout d'un sous-réseau ou d'un serveur Web dans l'environnement). Ces tests de pénétration doivent inclure ce qui suit :</p> <ul style="list-style-type: none"> 11.3.1 Tests de pénétration de la couche Réseau 11.3.2 Tests de pénétration de la couche Application 	<p>Les tests de pénétration des couches Réseau et Applications sont différents des analyses des vulnérabilités dans la mesure où les tests de pénétration sont davantage manuels, tentent d'exploiter véritablement certaines vulnérabilités identifiées pendant les analyses et comprennent des techniques employées par les individus malveillants pour tirer parti de la faiblesse des processus ou des systèmes de sécurité.</p> <p>Avant que des applications, des systèmes et des équipements réseau puissent être introduits dans l'environnement de production, ils doivent être renforcés et sécurisés au moyen des meilleures pratiques en matière de sécurité (conformément à l'exigence 2.2). Les analyses des vulnérabilités et les tests de pénétration mettront à nu toutes les autres vulnérabilités susceptibles d'être détectées et exploitées ultérieurement par un pirate.</p>

Exigence	Directive
<p>11.4 Utiliser des systèmes de détection d'intrusions et/ou des systèmes de prévention d'intrusions pour contrôler l'intégralité du trafic dans l'environnement des données de titulaire de carte et signaler au personnel tous les soupçons portant sur des altérations potentielles. Tenir à jour tous les moteurs de détection et de prévention des intrusions.</p>	<p>Ces outils comparent le trafic entrant sur le réseau aux « signatures » connues de milliers de types de violations (outils de piratage, chevaux de Troie et autres programmes malveillants), envoient des alertes et/ou bloquent la tentative. En l'absence d'une approche proactive de la détection des activités non autorisées à l'aide de ces outils, les attaques (ou la manipulation frauduleuse) des ressources d'un ordinateur pourraient passer inaperçues lorsqu'elles se produisent. Les alertes de sécurité générées par ces outils doivent être contrôlées de sorte que les tentatives d'intrusion puissent être bloquées.</p> <p>Il existe des milliers de types de violations et chaque jour on en découvre des nouvelles. Les anciennes versions de ces systèmes ne comprendront pas les « signatures » les plus actuelles et, par conséquent, n'identifieront pas les nouvelles vulnérabilités susceptibles d'entraîner des violations non détectées. Les fournisseurs de ces produits publient régulièrement, souvent quotidiennement, des mises à jour.</p>
<p>11.5 Déployer des logiciels de contrôle de l'intégrité des fichiers pour signaler au personnel toute modification non autorisée des fichiers de configuration, des fichiers de contenu ou des fichiers système stratégiques, et configurer ces logiciels pour effectuer des comparaisons entre les fichiers stratégiques au moins une fois par semaine.</p> <p><i>Remarque : Pour le contrôle de l'intégrité des fichiers, les fichiers stratégiques sont généralement ceux qui ne changent pas régulièrement, mais dont la modification pourrait indiquer une altération du système ou son exposition à des risques. Les produits de contrôle de l'intégrité des fichiers sont généralement préconfigurés avec les fichiers stratégiques pour le système d'exploitation associé. D'autres fichiers stratégiques, tels que ceux associés aux applications personnalisées, doivent être évalués et définis par l'entité (c'est-à-dire le commerçant ou le prestataire de services).</i></p>	<p>Les systèmes de contrôle de l'intégrité des fichiers (FIM) vérifient et signalent les modifications apportées aux fichiers stratégiques. Des outils prêts à l'emploi ainsi que des outils à code source libre sont disponibles pour le contrôle de l'intégrité des fichiers. Si ces systèmes ne sont pas correctement mis en œuvre et leurs résultats contrôlés, un individu malveillant pourrait modifier le contenu des fichiers de configuration, les programmes du système d'exploitation ou les fichiers exécutables des applications. Ces modifications non autorisées, si elles ne sont pas détectées, peuvent rendre les contrôles de sécurité inutiles et/ou entraîner le vol des données de titulaire de carte sans que le moindre impact soit perceptible au niveau du traitement normal.</p>

Directives relatives à l'exigence 12 : Gestion d'une politique de sécurité des informations

Exigence 12 : Gérer une politique qui assure la sécurité des informations des employés et des sous-traitants

Une politique de sécurité solide définit la sécurité mise en œuvre à l'échelle de l'entreprise et indique aux employés ce qu'on attend d'eux. Tous les employés doivent être sensibilisés au caractère confidentiel des données et à leurs responsabilités dans la protection de ces informations. Dans le cadre de cette exigence, le terme « employés » désigne les employés à temps plein et à temps partiel, les employés et le personnel intérimaires ainsi que les sous-traitants et les consultants qui « résident » sur le site de la société.

Exigence	Directive
<p>12.1 Définir, publier, gérer et diffuser une politique de sécurité qui remplit les fonctions suivantes :</p> <p>12.1.1 Satisfait toutes les exigences des normes PCI DSS.</p> <p>12.1.2 Inclut un processus annuel qui identifie les menaces et les vulnérabilités, et débouche sur une évaluation formelle des risques.</p> <p>12.1.3 Comprend au moins un examen annuel et est mise à jour chaque fois que l'environnement change.</p>	<p>La politique de sécurité des informations d'une entreprise définit la feuille de route à suivre pour mettre en œuvre les mesures de sécurité visant à protéger ses ressources les plus précieuses. Une politique de sécurité solide définit la sécurité mise en œuvre à l'échelle de l'entreprise et indique aux employés ce qu'on attend d'eux. Tous les employés doivent être sensibilisés au caractère confidentiel des données et à leurs responsabilités dans la protection de ces informations.</p> <p>Les menaces concernant la sécurité et les méthodes de protection changent rapidement tout au long de l'année. Sans la mise à jour de la politique de sécurité en vue de refléter ces changements, les nouvelles mesures de protection contre ces menaces seront vaines.</p>
<p>12.2 Élaborer des procédures de sécurité opérationnelles quotidiennes conformes aux exigences de cette spécification (par exemple, des procédures de gestion des comptes d'utilisateur et des procédures d'examen des journaux).</p>	<p>Les procédures de sécurité opérationnelles quotidiennes font office « d'instructions usuelles » que les employés doivent respecter dans le cadre de leurs activités quotidiennes liées à l'administration et la maintenance des systèmes. Si les procédures de sécurité opérationnelles ne sont pas documentées, les employés ne connaîtront pas la portée globale de leurs tâches, les processus ne pourront pas être reproduits facilement par les nouvelles recrues et des lacunes pourront apparaître dans ces processus, dont des individus malveillants pourraient tirer parti pour accéder aux ressources et aux systèmes stratégiques.</p>

Exigence	Directive
<p>12.3 Élaborer les politiques d'utilisation des technologies orientées employés stratégiques (par exemple, technologies d'accès à distance, technologies sans fil, supports électroniques amovibles, ordinateurs portables, assistants numériques personnels (PDA), utilisation du courrier électronique et utilisation d'Internet) pour définir l'usage approprié de ces technologies par tous les employés et les sous-traitants. S'assurer que ces politiques d'utilisation exigent ce qui suit :</p>	<p>Les politiques d'utilisation par les employés peuvent interdire l'usage de certains équipements et d'autres technologies si la politique de la société le stipule, ou orienter les employés quant à l'usage et l'implémentation appropriés de ces éléments. En l'absence de politiques d'utilisation, les employés peuvent utiliser les technologies contrevenant à la politique de la société, permettant ainsi à des individus malveillants d'accéder aux systèmes stratégiques et aux données de titulaire de carte. Par exemple, ils peuvent configurer sans le savoir des réseaux sans fil n'intégrant aucun mécanisme de sécurité. Pour veiller à ce que les règles de l'entreprise soient respectées et que seules les technologies approuvées soient déployées, envisagez de restreindre l'implémentation aux équipes d'exploitation et d'interdire à tout employé non spécialisé/ordinaire d'installer ces technologies.</p>
<p>12.3.1 Approbation explicite des responsables</p>	<p>Si l'implémentation de ces technologies n'est pas correctement approuvée par les responsables, un employé peut, en toute innocence, installer une solution dont il pense avoir besoin, causant alors une faille importante qui expose les données et les systèmes stratégiques à des individus malveillants.</p>
<p>12.3.2 Authentification de l'utilisation des technologies</p>	<p>Si la technologie est mise en œuvre sans une authentification appropriée (ID utilisateur et mots de passe, jetons, VPN, etc.), des individus malveillants pourraient facilement utiliser cette technologie non protégée pour accéder aux systèmes stratégiques et aux données de titulaire de carte.</p>
<p>12.3.3 Liste de tous les périphériques et employés disposant d'un accès</p>	<p>Des individus malveillants peuvent violer la sécurité physique et placer leurs propres équipements sur le réseau en tant que « porte dérobée ». Les employés peuvent également contourner des procédures et installer des équipements. L'inventaire précis des équipements, qui doivent être correctement étiquetés, permet d'identifier rapidement les installations non approuvées. Envisagez de définir une convention de dénomination officielle des équipements et de tous les étiqueter et les consigner parallèlement aux contrôles d'inventaires mis en place.</p>
<p>12.3.4 Indication sur les périphériques du nom de leurs propriétaires, de leurs coordonnées et de leur usage</p>	
<p>12.3.5 Usages acceptables des technologies</p>	<p>En définissant l'usage professionnel acceptable et l'emplacement des équipements et des technologies de l'entreprise, cette dernière pourra mieux gérer et contrôler les failles au niveau des configurations et des contrôles opérationnels, afin de s'assurer qu'aucune « porte dérobée » n'est ouverte pour permettre l'accès d'un individu malveillant aux systèmes stratégiques et aux données de titulaire de carte.</p>
<p>12.3.6 Emplacements acceptables des technologies sur le réseau</p>	
<p>12.3.7 Liste des produits approuvés par l'entreprise</p>	

Exigence	Directive
<p>12.3.8 Déconnexion automatique des sessions des technologies d'accès à distance après une période d'inactivité spécifique</p>	<p>Les technologies d'accès à distance sont des « portes dérobées » fréquentes permettant d'accéder aux ressources stratégiques et aux données de titulaire de carte. En déconnectant ces technologies lorsqu'elles ne sont pas utilisées (par exemple, celles utilisées pour la maintenance de vos systèmes par vos fournisseurs de points de vente et autres), vous réduisez les risques d'accès à votre réseau. Envisagez la mise en place de contrôles pour déconnecter les équipements restés inactifs pendant 15 minutes. Reportez-vous également à l'exigence 8.5.6 pour plus d'informations à ce sujet.</p>
<p>12.3.9 Activation des technologies d'accès à distance pour les fournisseurs strictement lorsque cela est nécessaire et désactivation immédiate de cet accès après usage</p>	
<p>12.3.10 Lors de l'accès aux données de titulaire de carte au moyen de technologies d'accès à distance, interdire la copie, le déplacement et le stockage de données de titulaire de carte sur des disques durs locaux et des supports électroniques amovibles.</p>	
<p>12.4 S'assurer que la politique et les procédures de sécurité définissent clairement les responsabilités de tous les employés et sous-traitants en matière de sécurité des informations.</p>	<p>En l'absence d'une définition claire des responsabilités et des rôles en matière de sécurité, l'interaction avec le groupe en charge de la sécurité peut être incohérente, conduisant alors au déploiement de technologies non sécurisées ou à l'usage de technologies obsolètes ou impliquant des risques.</p>
<p>12.5 Attribuer à un individu ou à une équipe les responsabilités suivantes de gestion de la sécurité des informations :</p> <ul style="list-style-type: none"> 12.5.1 Définir, documenter et diffuser les politiques et les procédures de sécurité. 12.5.2 Contrôler et analyser les informations et les alertes de sécurité, et les diffuser au personnel compétent. 12.5.3 Définir, documenter et diffuser les procédures d'escalade et de réponse aux incidents liés à la sécurité pour garantir une gestion rapide et efficace de toutes les situations. 12.5.4 Administrer les comptes d'utilisateur, notamment l'ajout, la suppression et la modification de comptes 12.5.5 Surveiller et contrôler tous les accès aux données. 	<p>Chaque individu ou équipe responsable de la gestion de la sécurité des informations doit connaître parfaitement ses responsabilités et les tâches associées, par le biais d'une politique spécifique. Sans cette responsabilisation, les lacunes dans les processus peuvent permettre l'accès d'intrus aux ressources stratégiques et aux données de titulaire de carte.</p>

Exigence	Directive
<p>12.6 Mettre en œuvre un programme formel de sensibilisation à la sécurité pour sensibiliser les employés à l'importance de la sécurité des données de titulaire de carte.</p>	<p>Si les utilisateurs ne sont pas sensibilisés à leurs responsabilités en matière de sécurité, les processus et les mesures mis en place peuvent s'avérer inefficaces compte tenu des erreurs que les employés peuvent commettre ou de leurs actions délibérées.</p>
<p>12.6.1 Sensibiliser les employés au moment de leur recrutement et au moins une fois par an.</p>	<p>Si le programme de sensibilisation à la sécurité ne prévoit pas des sessions d'actualisation annuelles, les principaux processus et procédures en matière de sécurité pourront être oubliés ou ignorés, entraînant alors l'exposition des ressources stratégiques et des données de titulaire de carte à des risques.</p>
<p>12.6.2 Exiger que les employés reconnaissent au moins une fois par an avoir lu et compris les procédures et la politique de sécurité de la société.</p>	<p>Exiger une reconnaissance par les employés (par exemple, par écrit ou par e-mail) vous permet de vous assurer qu'ils ont bien lu et compris les politiques et procédures en matière de sécurité, et qu'ils s'engagent à les respecter.</p>
<p>12.7 Passer au crible les employés potentiels (voir la définition du terme « employé » au point 9.2 ci-dessus) avant leur recrutement afin de réduire les risques d'attaques depuis des sources internes. <i>Pour les employés tels que les caissiers dans les magasins, qui n'ont accès qu'à un numéro de carte à la fois à l'occasion du traitement d'une transaction, cette exigence n'est qu'une recommandation.</i></p>	<p>La vérification détaillée des renseignements concernant les employés qui auront accès aux données de titulaire de carte avant leur recrutement réduit les risques d'utilisations non autorisées des PAN et autres données de titulaire de carte par des individus qui ne seraient pas dignes de confiance. Il est attendu d'une entreprise qu'elle dispose d'une politique et d'un processus de vérification des renseignements concernant les employés, notamment son propre processus de décision quant aux résultats de ces vérifications qui affecteraient ses décisions de recrutement (et détermineraient le type d'impact).</p>
<p>12.8 Si les données de titulaire de carte sont partagées avec des prestataires de services, gérer et mettre en œuvre les politiques et les procédures de gestion de ces derniers, de manière à inclure :</p>	<p>Si un commerçant ou un prestataire de services partage les données de titulaire de carte avec un autre prestataire de services, certaines exigences s'appliquent alors pour veiller à la protection permanente de ces informations par les deux parties.</p>
<p>12.8.1 Tenir la liste des prestataires de services.</p>	<p>Connaître les prestataires de services permet d'identifier les risques potentiels à l'extérieur de l'entreprise.</p>
<p>12.8.2 Faire signer aux prestataires de services un accord écrit par lequel ils se reconnaissent responsables de la sécurité des données de titulaire de carte en leur possession.</p>	<p>Par la signature de l'accord, les prestataires de services reconnaissent qu'ils s'engagent à assurer de manière adéquate la sécurité des données de titulaire de carte qu'ils obtiennent auprès de leurs clients, et qu'ils en sont responsables.</p>
<p>12.8.3 S'assurer que le processus de sélection des prestataires de services est bien défini, et qu'il inclut notamment des contrôles préalables au recrutement.</p>	<p>Ce processus garantit que la sélection de tout prestataire de services est parfaitement évaluée en interne par l'entreprise, et que l'initiation de toute relation formelle avec ce prestataire a été précédée d'une analyse des risques.</p>

Exigence	Directive
<p>12.8.4 Mettre en place un programme qui contrôle la conformité des prestataires de services avec les normes PCI DSS.</p>	<p>Connaître la conformité d'un prestataire de services avec les normes PCI DSS garantit encore mieux qu'il respecte les mêmes exigences que celles de l'entreprise.</p>
<p>12.9 Mettre en œuvre un plan de réponse aux incidents. Être prêt à réagir immédiatement à toute intrusion dans le système.</p>	<p>En l'absence d'un plan de réponse aux incidents détaillé, qui soit correctement diffusé, lu et compris par les parties responsables, il peut régner une certaine confusion et l'absence de réponses unifiées, qui peuvent perturber encore plus le fonctionnement de l'entreprise, et entraîner une exposition publique des supports superflue et de nouvelles responsabilités civiles.</p>
<p>12.9.1 Créer le plan de réponse aux incidents à mettre en œuvre en cas d'intrusion dans le système. S'assurer que le plan prévoit au moins les points suivants :</p> <ul style="list-style-type: none"> ▪ Rôles, responsabilités et stratégies de communication et de contact en cas d'incident, notamment notification des marques de cartes de paiement, au minimum ▪ Procédures de réponse aux incidents spécifiques ▪ Procédures de continuité et de reprise des affaires ▪ le processus de sauvegarde des données ; ▪ Analyse des exigences légales en matière de signalement des incidents ▪ Couverture et réponses de tous les composants stratégiques du système ▪ la référence ou l'inclusion des procédures de réponse aux incidents des marques de cartes de paiement. 	<p>Le plan de réponse aux incidents doit être détaillé et doit contenir les éléments clés permettant à l'entreprise de réagir efficacement en cas de violation susceptible d'affecter les données de titulaire de carte.</p>

Exigence	Directive
<p>12.9.2 Tester le plan au moins une fois par an.</p>	<p>En l'absence de tests appropriés, des étapes importantes susceptibles de limiter l'exposition en cas d'incident risquent d'être négligées.</p>
<p>12.9.3 Désigner le personnel spécifique disponible 24 heures sur 24 et sept jours sur sept pour répondre aux alertes.</p>	<p>En l'absence d'une équipe de réponse aux incidents bien formée et disponible à tout moment, des dégâts importants peuvent être causés sur le réseau, et les données et les systèmes stratégiques peuvent être altérés par la manipulation inappropriée des systèmes visés. Cela peut entraver l'aboutissement de l'enquête réalisée après un incident. Si vous ne possédez pas de ressources internes, envisagez la sous-traitance de ce service auprès d'un prestataire compétent.</p>
<p>12.9.4 Organiser la formation appropriée du personnel en charge de la réponse aux violations de la sécurité.</p>	
<p>12.9.5 Inclure des alertes des systèmes de détection et de prévention des intrusions, et de contrôle de l'intégrité des fichiers.</p>	<p>Ces systèmes de contrôle sont conçus pour mettre l'accent sur les risques potentiels encourus par les données. Ils sont essentiels pour agir rapidement en vue de prévenir une violation et ils doivent être intégrés aux processus de réponse aux incidents.</p>
<p>12.9.6 Définir un processus de modification et de développement du plan de réponse aux incidents en fonction des leçons apprises, et tenir compte de l'évolution du secteur.</p>	<p>L'intégration des « leçons apprises » au plan de réponse aux incidents après un problème permet de tenir à jour ce plan et de réagir face aux nouvelles menaces et tendances en matière de sécurité.</p>

Directives relatives à l'exigence A.1 : Autres exigences des normes PCI DSS s'appliquant aux fournisseurs d'hébergement partagé

Exigence A.1 : Les prestataires de services d'hébergement partagé protègent l'environnement des données de titulaire de carte

Comme indiqué dans l'exigence 12.8, tous les prestataires de services qui ont accès aux données de titulaire de carte (notamment les prestataires de services d'hébergement partagé) doivent respecter les normes PCI DSS. En outre, l'exigence 2.4 stipule que les prestataires de services d'hébergement partagé doivent protéger les données et l'environnement hébergés de chaque entité. En conséquence, les prestataires de services d'hébergement partagé doivent par ailleurs se conformer aux exigences définies dans cette annexe.

Exigence	Directive
<p>A.1 Protéger les données et l'environnement hébergés de chaque entité (c'est-à-dire le commerçant, le prestataire de services ou toute autre entité), conformément aux exigences A.1.1 à A.1.4 :</p> <p>Un prestataire de services d'hébergement doit satisfaire à ces exigences ainsi qu'aux conditions de toutes les autres sections pertinentes des normes PCI DSS.</p> <p><i>Remarque : Même si un prestataire de services d'hébergement peut satisfaire ces exigences, le respect par l'entité qui a recours au prestataire de services d'hébergement n'est pas garanti.</i> Chaque entité doit se conformer aux normes PCI DSS et doit valider cette conformité comme applicable.</p>	<p>L'annexe A des normes PCI DSS est destinée aux prestataires de services d'hébergement partagé qui souhaitent mettre à la disposition de leurs clients commerçants et/ou prestataires de services un environnement d'hébergement conforme à ces normes. Ces étapes doivent être satisfaites, de même que toutes les autres exigences pertinentes des normes PCI DSS.</p>
<p>A.1.1 S'assurer que chaque entité ne met en œuvre que les processus qui ont accès à l'environnement des données de titulaire de carte qui la concerne.</p>	<p>Si un commerçant ou un prestataire de services est autorisé à exécuter ses propres applications sur le serveur partagé, il doit utiliser l'ID utilisateur du commerçant ou du prestataire de services, et non un ID utilisateur privilégié. Un utilisateur privilégié peut accéder aux environnements des données de titulaire de carte de tous les autres commerçants et prestataires de services ainsi qu'au sien.</p>

Exigence	Directive
<p>A.1.2 Restreindre l'accès et les privilèges de chaque entité à son propre environnement de données de titulaire de carte.</p>	<p>Pour vous assurer que l'accès et les privilèges sont restreints de sorte que chaque commerçant et prestataire de services ne puisse accéder qu'à son propre environnement de données de titulaire de carte, prévoyez ce qui suit : (1) les privilèges de l'ID utilisateur du serveur Web du commerçant ou du prestataire de services ; (2) les permissions accordées pour la lecture, l'écriture et l'exécution de fichiers ; (3) les permissions accordées pour l'accès en écriture aux fichiers binaires du système ; (4) les permissions accordées pour l'accès aux fichiers journaux du commerçant et du prestataire de services ; et (5) des contrôles visant à s'assurer qu'aucun commerçant ou prestataire de services ne pourra monopoliser les ressources système.</p>
<p>A.1.3 S'assurer que la journalisation et les journaux d'audit sont activés, uniques à l'environnement des données de titulaire de carte de chaque entité et conformes à l'exigence 10 des normes PCI DSS.</p>	<p>Des journaux doivent être disponibles dans un environnement d'hébergement partagé de sorte que les commerçants et les prestataires de services puissent accéder aux journaux spécifiques à leur environnement de données de titulaire de carte afin de les passer en revue.</p>
<p>A.1.4 Activer les processus d'investigation légale rapide en cas d'incident dans l'environnement d'un commerçant ou d'un prestataire de services.</p>	<p>Les prestataires de services d'hébergement partagé doivent avoir des processus permettant une réponse rapide et simple en cas d'investigation légale suite à un incident, et permettant d'accéder au niveau de détail approprié.</p>

Annexe A : Normes PCI DSS : documents connexes

Les documents suivants visent à aider les commerçants et les prestataires de services à comprendre les normes PCI DSS, ainsi que les exigences et les responsabilités en matière de conformité.

Document	Public
<i>Normes de sécurité des données de la PCI : Conditions et procédures d'évaluation de sécurité</i>	Tous les commerçants et prestataires de services
<i>Navigation dans les normes PCI DSS : Comprendre l'objectif des exigences</i>	Tous les commerçants et prestataires de services
<i>Normes de sécurité des données de la PCI : Instructions et directives sur l'auto-évaluation</i>	Tous les commerçants et prestataires de services
<i>Normes de sécurité des données de la PCI : Questionnaire d'auto-évaluation A et attestation</i>	Commerçants ¹⁰
<i>Normes PCI DSS : Questionnaire d'auto-évaluation B et attestation</i>	Commerçants ¹⁰
<i>Normes PCI DSS : Questionnaire d'auto-évaluation C et attestation</i>	Commerçants ¹⁰
<i>Normes PCI DSS : Questionnaire d'auto-évaluation D et attestation</i>	Commerçants ¹⁰ et tous les prestataires de services
<i>Glossaire des termes, abréviations et acronymes PCI DSS et PA-DSS</i>	Tous les commerçants et prestataires de services

¹⁰ Pour déterminer le questionnaire d'auto-évaluation approprié, voir *Normes de sécurité des données de la PCI : Instructions et directives sur l'auto-évaluation*, « Sélection du questionnaire d'auto-évaluation et de l'attestation les plus appropriés pour votre entreprise ».