



PCI DSS et les produits de Sécurité de Réseau de GFI

Conditions PCI DSS	ESM 7	LANSS 8
Condition 1: Installer et maintenir une configuration de pare-feu pour protéger les données de propriétaires de carte		
1.3 Etablir une configuration de pare-feu pour limiter l'accès aux données de propriétaires de cartes		
1.3.1 Limiter le trafic internet entrant aux adresses IP se trouvant dans la zone démilitarisée	●	
1.3.6 Sécuriser et synchroniser les fichiers de configuration de routeur	●	
1.3.7 Interdire tout autre trafic entrant ou sortant qui n'est pas spécifiquement autorisé	●	
1.3.9 Installer un logiciel pare-feu personnel sur les ordinateurs portables ou appartenant aux employés ayant une connectivité directe à Internet, qui sont utilisés pour accéder au réseau d'une organisation.		✓
Condition 2: Ne pas utiliser de mots de passe créés par les fournisseurs		
2.1 Modifier toujours les paramètres par défaut créés par les fournisseurs avant d'installer un système sur un réseau		
2.2 Etablir des normes de configuration pour tous les composants d'un système		
2.2.2 Désactiver tous les services et protocoles non sécurisés	●	●
2.2.3 Configurer les paramètres de sécurité de système pour empêcher l'abus		●
2.2.4 Supprimer toute fonctionnalité inutile tels que les scripts, les pilotes, les serveurs web, etc.		●
Condition 3: Protéger les données stockées des propriétaires de cartes		
3.5 Protéger les clés utilisées pour le chiffage des données de propriétaires de carte contre la divulgation et l'abus		
3.5.1 Limiter l'accès aux clés à un nombre minimum possible de personnes	●	
3.6 Classer et mettre en application systématiquement tous les processus et procédures de gestion des clés utilisées pour le chiffage des données de propriétaires de cartes		
3.6.3 Sécuriser le stockage des clés	●	
Condition 5: Utiliser et régulièrement mettre à niveau les programmes et logiciels anti-virus		
5.1 Déployer des logiciels anti-virus sur tous les systèmes communément affectés par les virus		
5.2 Assurer que tous les mécanismes anti-virus sont activés et fonctionnent correctement		
Condition 6: Etablir et maintenir des systèmes et des applications sécurisés		
6.1 Assurer l'installation des plus récents patches de sécurité pour tous les composants des systèmes et les logiciels		
6.2 Etablir un processus d'identification des vulnérabilités de sécurité nouvellement découvertes		
6.4 Suivre des procédures de contrôle pour toute modification de configuration des systèmes et des logiciels		
6.4.3 Tester que les fonctionnalités sont opérationnelles		✓
6.5 Développer toutes les applications web selon des critères de programmation privilégiant la sécurité		
6.6 Assurer que les applications d'interface avec le web sont protégées contre les attaques connues en installant une application de pare-feu		
Condition 7: Limiter l'accès aux données de propriétaires de cartes au personnel approprié de l'entreprise		
7.1 Limiter l'accès aux ressources informatiques et aux détails des propriétaires de cartes aux seuls individus dont le travail nécessite un tel accès		
7.2 Etablir un mécanisme pour les systèmes avec les utilisateurs multiples qui limite l'accès selon le besoin d'utilisateur et empêche tout accès qui n'est pas spécifiquement autorisé		
Condition 8: Assigner une identification unique à chaque personne ayant l'accès par ordinateur		
8.2 Assigner des identifications et des mots de passe uniques		
8.5 Assurer l'authentification et la gestion appropriées d'utilisateur et de mots de passe de tout le personnel		
8.5.1 Contrôler l'ajout, la suppression ou la modification des paramètres d'identification	●	
8.5.2 Vérifier l'identité d'utilisateur avant d'effectuer l'initialisation des mots de passe	●	
8.5.3 Assigner aux utilisateurs un mot de passe unique d'accès qui est modifié suite après le premier usage	●	●
8.5.4 Retirer immédiatement le droit d'accès à tous les utilisateurs révoqués	●	
8.5.5 Supprimer les comptes d'utilisateur inactifs, au moins tous les 90 jours	●	●
8.5.6 Activer seulement quand c'est nécessaire, les comptes utilisés par les distributeurs pour l'entretien à distance	●	●

Conditions PCI DSS	ESM 7	LANSS 8
8.5.9 Changer les mots de passe d'utilisateur au moins tous les 90 jours		●
8.5.10 Exiger une longueur minimum de mot de passe d'au moins sept caractères		●
8.5.13 Limiter à six, les tentatives d'accès répétées, par le blocage de l'utilisateur	●	
8.5.16 Authentifier tous les accès à toute base de données contenant des données de propriétaires de carte	●	
Condition 10: Traquer et surveiller tous les accès aux ressources de réseau et aux données de propriétaires de carte		
10.1 Enregistrer tous les accès individuels des utilisateurs aux composants du système, en particulier les administrateurs	●	
10.2 Activer la vérification rétrospective automatique de tout le système pour reconstituer les événements suivants:		
10.2.1 Tous les accès individuels aux données de propriétaires de carte	●	
10.2.2 Toutes les mesures prises par un individu ayant des droits d'accès 'root' ou d'administrateur	✓	
10.2.3 Accès à toutes les vérifications rétrospectives	✓	
10.2.4 Tentatives d'accès invalides	✓	
10.2.5 Utilisation des mécanismes d'identification et d'authentification	✓	
10.2.6 Initialisation des enregistrements des vérifications	✓	
10.2.7 Création et suppression d'éléments au niveau du système	✓	
10.3 Enregistrer les détails d'apurement de tous les événements liés aux composants du système	✓	
10.4 Synchroniser toutes les principales horloges et l'heure du système	●	●
10.5 Sécuriser les dossiers d'apurement afin qu'ils ne puissent pas être modifiés		
10.5.1 Limiter l'accès et l'affichage dossiers de vérification à ceux dont la tâche l'exige	●	
10.5.2 Protéger les fichiers d'apurement contre les modifications non autorisées	●	
10.5.5 Utiliser un logiciel de contrôle de l'intégrité et de détection de changements pour assurer que les données ne peuvent pas être modifiées (sauf pour les nouvelles données) sans générer d'alertes	✓	
10.6 Passer en revue, au moins chaque jour, les enregistrements de tous les composants de système	✓	
Condition 11: Tester régulièrement la sécurité des systèmes et des processus		
11.1 Tester les fonctions de sécurité, les restrictions, les connexions et les restrictions d'accès de réseau pour assurer la capacité d'identifier adéquatement et d'arrêter toutes tentatives d'accès non autorisé	●	✓
11.2 Effectuer des balayages internes de vulnérabilité de réseau au moins une fois par trimestre		✓
11.4 Utiliser des systèmes de détection d'intrusion de réseau, des systèmes de détection d'intrusion sur les machines hôtes et des systèmes de prévention d'intrusion	●	●
11.5 Déployer un logiciel de contrôle de l'intégrité des fichiers pour envoyer des alertes en cas de modifications non autorisées du système central ou du contenu des fichiers	✓	✓

Légende

- ✓ Condition entièrement supportée
- Condition supportée partiellement grâce au rapports ou à une adaptation du produit. Certaines conditions pourraient s'appliquer

REMARQUE: Les conditions applicables incluent mais ne sont pas limitées à :

- Windows Security Settings, tels que 'Password Policy' et 'Audit Policy'
- Paramétrages de compte utilisateur
- Installation et configuration appropriée d'autres logiciels et dispositifs, tels que des pare-feu

