



GFI PCI DSS and GFI Network Security products

PCI DSS requirements	ESM 7	LANSS 8
Requirement 1: Install and maintain a firewall configuration to protect cardholder data		
1.3 Build a firewall configuration to restrict connections to cardholder data		
1.3.1 Restricting inbound Internet traffic to IP addresses within the DMZ	●	
1.3.6 Securing and synchronizing router configuration files	●	
1.3.7 Denying all other inbound and outbound traffic not specifically allowed	●	
1.3.9 Install personal firewall software on mobile and employee-owned computers with direct connectivity to the Internet, used to access the organization's network		✓
Requirement 2: Do not use vendor-supplied default passwords		
2.1 Always change vendor-supplied defaults before installing a system on the network		●
2.2 Develop configuration standards for all system components		
2.2.2 Disable all unnecessary and insecure services and protocols	●	●
2.2.3 Configure system security parameters to prevent misuse		●
2.2.4 Remove all unnecessary functionality, such as scripts, drivers, web servers		●
Requirement 3: Protect stored cardholder data		
3.5 Protect encryption keys used for encryption of cardholder data against both disclosure and misuse		
3.5.1 Restrict access to keys to the fewest number of custodians necessary	●	
3.6 Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data		
3.6.3 Secure key storage	●	
Requirement 5: Use and regularly update anti-virus software or programs		
5.1 Deploy anti-virus software on all systems commonly affected by viruses		✓
5.2 Ensure that all anti-virus mechanisms are current, actively running		✓
Requirement 6: Develop and maintain secure systems and applications		
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed		✓
6.2 Establish a process to identify newly discovered security vulnerabilities		✓
6.4 Follow change control procedures for all system and software configuration changes		
6.4.3 Testing of operational functionality		✓
6.5 Develop all web applications based on secure coding guidelines		●
6.6 Ensure that all web-facing applications are protected against known attacks by installing an application-layer firewall		✓
Requirement 7: Restrict access to cardholder data by business need-to-know		
7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access	●	
7.2 Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed	●	
Requirement 8: Assign a unique ID to each person with computer access		
8.2 Assign unique IDs, and passwords		●
8.5 Ensure proper user authentication and password management for non-consumer users and administrators		
8.5.1 Control addition, deletion, or modification of user IDs, credentials, and other identifier objects	●	
8.5.2 Verify user identity before performing password resets	●	
8.5.3 Set first-time passwords to a unique value for each user and change immediately after first use	●	●
8.5.4 Immediately revoke access for any terminated users	●	
8.5.5 Remove inactive user accounts at least every 90 days	●	●
8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed	●	●

PCI DSS requirements	ESM 7	LANSS 8
8.5.9 Change user passwords at least every 90 days		●
8.5.10 Require a minimum password length of at least seven characters		●
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts	●	
8.5.16 Authenticate all access to any database containing cardholder data	●	
Requirement 10: Track and monitor all access to network resources and cardholder data		
10.1 Log all individual user access to system components, especially administrative users	●	
10.2 Implement automated audit trails for all system components to reconstruct the following events:		
10.2.1 All individual accesses to cardholder data	●	
10.2.2 All actions taken by any individual with root or administrative privileges	✓	
10.2.3 Access to all audit trails	✓	
10.2.4 Invalid logical access attempts	✓	
10.2.5 Use of identification and authentication mechanisms	✓	
10.2.6 Initialization of the audit logs	✓	
10.2.7 Creation and deletion of system- level objects	✓	
10.3 Record audit trail details for all system component related events	✓	
10.4 Synchronize all critical system clocks and times	●	●
10.5 Secure audit trails so they cannot be altered		
10.5.1 Limit viewing of audit trails to those with a job-related need	●	
10.5.2 Protect audit trail files from unauthorized modifications	●	
10.5.5 Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed (except for new data) without generating alerts	✓	
10.6 Review logs for all system components at least daily	✓	
Requirement 11: Regularly test security systems and processes		
11.1 Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts	●	✓
11.2 Run internal and external network vulnerability scans at least quarterly		✓
11.4 Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises	●	●
11.5 Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files	✓	✓

Legend

- ✓ Requirement fully supported
- Requirement partially supported through reporting or product customization. Certain conditions may apply.

Note: Conditions apply which include, but are not limited to:

- Windows Security Settings, such as Password Policy and Audit Policy
- User account settings
- Third-party software and devices, such as firewalls, being properly installed and configured

