



# GFI PCI DSS and GFI LANguard N.S.S. 8

| PCI DSS requirements   | Auditing | Monitoring and reporting | Alerting | Enforcing | Notes                             |
|--|----------|--------------------------|----------|-----------|-----------------------------------|
| <b>Requirement 1: Install and maintain a firewall configuration to protect cardholder data</b>   |          |                          |          |           |                                   |
| <b>1.3</b> Build a firewall configuration to restrict connections to cardholder data   |          |                          |          |           |                                   |
| <b>1.3.9</b> Install personal firewall software on mobile and employee-owned computers with direct connectivity to the Internet, used to access the organization's network | ✓        | ✓                        | ●        | ✓         | Default scan profiles and reports |
| <b>Requirement 2: Do not use vendor-supplied default passwords</b>   |          |                          |          |           |                                   |
| <b>2.1</b> Always change vendor-supplied defaults before installing a system on the network  | ●        | ✓                        | ●        |           | Default scan profiles and reports |
| <b>2.2</b> Develop configuration standards for all system components; address all known security vulnerabilities   |          |                          |          |           |                                   |
| <b>2.2.2</b> Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)           | ✓        | ✓                        | ●        |           | Default scan profiles and reports |
| <b>2.2.3</b> Configure system security parameters to prevent misuse  | ✓        | ✓                        | ●        |           | Default scan profiles and reports |
| <b>2.2.4</b> Remove all unnecessary functionality, such as scripts, drivers, web servers   | ✓        | ✓                        | ●        |           | Default scan profiles and reports |
| <b>Requirement 5: Use and regularly update anti-virus software or programs</b>   |          |                          |          |           |                                   |
| <b>5.1</b> Deploy anti-virus software on all systems commonly affected by viruses  | ✓        | ✓                        | ●        | ✓         | Default scan profiles and reports |
| <b>5.2</b> Ensure that all anti-virus mechanisms are current, actively running   | ✓        | ✓                        | ●        | ✓         | Default scan profiles and reports |
| <b>Requirement 6: Develop and maintain secure systems and applications</b>   |          |                          |          |           |                                   |
| <b>6.1</b> Ensure that all system components and software have the latest vendor-supplied security patches installed   | ✓        | ✓                        | ●        | ✓         | Default scan profiles and reports |
| <b>6.2</b> Establish a process to identify newly discovered security vulnerabilities   | ✓        | ✓                        | ●        | ✓         | Schedule network audits           |
| <b>6.4</b> Follow change control procedures for all system and software configuration changes  |          |                          |          |           |                                   |
| <b>6.4.3</b> Testing of operational functionality  | ✓        | ✓                        | ●        | ✓         | Patch deployment rollback         |
| <b>6.5</b> Develop all web applications based on secure coding guidelines  | ✓        | ✓                        | ●        |           | OVAL vulnerability checks         |
| <b>6.6</b> Ensure that all web-facing applications are protected against known attacks by installing an application-layer firewall   | ✓        | ✓                        | ●        | ✓         | Default scan profiles and reports |
| <b>Requirement 8: Assign a unique ID to each person with computer access</b>   |          |                          |          |           |                                   |
| <b>8.2</b> Assign unique IDs and passwords   | ✓        | ✓                        | ●        |           | Default scan profiles and reports |
| <b>8.5</b> Ensure proper user authentication and password management   |          |                          |          |           |                                   |
| <b>8.5.3</b> Set first-time passwords to a unique value for each user and change immediately after first use   | ●        | ●                        | ●        |           | Default scan profiles and reports |
| <b>8.5.5</b> Remove inactive user accounts at least every 90 days  | ●        | ●                        | ●        |           | Default scan profiles and reports |
| <b>8.5.6</b> Enable accounts used by vendors for remote maintenance only during the time period needed   | ●        | ●                        | ●        |           | Default scan profiles and reports |

| PCI DSS requirements  | Auditing | Monitoring and reporting | Alerting | Enforcing | Notes                             |
|---|----------|--------------------------|----------|-----------|-----------------------------------|
| <b>8.5.9</b> Change user passwords at least every 90 days   | ✓        | ✓                        | ●        |           | Default scan profiles and reports |
| <b>8.5.10</b> Require a minimum password length of at least seven characters  | ✓        | ✓                        | ●        |           | Default scan profiles and reports |
| <b>Requirement 10: Track and monitor all access to network resources and cardholder data</b>  |          |                          |          |           |                                   |
| <b>10.4</b> Synchronize all critical system clocks and times  | ✓        | ✓                        | ●        |           | Default scan profiles and reports |
| <b>Requirement 11: Regularly test security systems and processes</b>  |          |                          |          |           |                                   |
| <b>11.1</b> Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts                 | ✓        | ✓                        | ●        | ✓         | Schedule network audits           |
| <b>11.2</b> Run internal and external network vulnerability scans at least quarterly  | ✓        | ✓                        | ●        | ✓         | Schedule network audits           |
| <b>11.4</b> 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 | ✓        | ✓                        | ●        |           | Default scan profiles and reports |
| <b>11.5</b> Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files   | ✓        | ✓                        | ●        | ✓         | Default scan profiles and reports |

#### 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

