

Testing of Networks

Approved By: <hr/> \\S\ James Palmer CSC Loss Prevention Director <hr/> December 31, 2014 Date	PCI Policy # 2100 Version # 1.0 Effective Date: 12/31/2014
---	--

1.0 Purpose:

The purpose is to implement policies and procedures to ensure that all access to network resources and cardholder data is regularly tested.

2.0 Compliance:

PCI DSS Requirement 11

3.0 Scope:

This policy applies to ABC COMPANY in its entirety, including all systems, network, and applications that process, store or transmit sensitive information.

4.0 Policy:

Procedures for security monitoring and testing will be documented, implemented and known to all affected parties.

Testing Policy

All security controls, limitations, network connections, and restrictions will be tested annually to assure the ability to adequately identify and to stop any unauthorized access attempts.

Approved wireless access testing methods include but are not limited to: physical/logical inspection of system components and infrastructure, use of network access control (NAC), and/or wireless IDS/IPS.

Wireless Testing

Procedures for the detection and identification of both authorized and unauthorized wireless access points on a quarterly basis will be documented and implemented. The procedures will include:

- Detection and identification of unauthorized wireless access points, including at least the following:
 - WLAN cards inserted into system components;
 - Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.)
 - Wireless devices attached to a network port or network device
- Reviewing wireless scans to verify:
 - Authorized and unauthorized wireless access points are identified
 - Scans are performed at least quarterly for all system components and facilities
- If automated monitoring is used (such as wireless IDS/IPS, NAC, etc.) it will be configured so that it generates alerts to personnel.

An inventory of authorized wireless access points including a documented business justification will be maintained.

Incident Response procedures in the event unauthorized wireless access points are detected will be documented and implemented.

Systems Testing

Internal and external network vulnerability scans will be run at least quarterly and after any significant change in the network. This includes rescans as needed until all “high” vulnerabilities are resolved. Rescans must be run by qualified personnel.

Quarterly external vulnerability scans must be performed by a scan vendor approved by the payment card industry. Scans conducted after network changes may be performed by ABC COMPANY’s internal staff.

Quarterly internal vulnerability scans include rescans as needed until all “high” vulnerabilities are resolved, and must be performed by qualified personnel.

A methodology for penetration testing will be documented and implemented. Methodology should include:

- Industry – accepted penetration testing approaches
- Coverage for the entire cardholder data environment perimeter and critical systems
- Testing from both inside and outside the network
- Testing to validate any segmentation and scope-reduction controls
- Application-layer penetration tests to include, at a minimum, the vulnerabilities in PCI DSS Requirement 6.5
- Network-layer penetration tests to include components that support network functions as well as operating systems
- Reviews and consideration of threats and vulnerabilities experienced in the last 12 months
- Retention of penetration testing results and remediation activities results

External penetration testing will be performed at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

Internal penetration testing will be performed at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

Exploitable vulnerabilities found during penetration testing will be corrected and testing will be repeated to verify corrections

If segmentation is used to isolate the cardholder data environment from other networks, penetration tests will be performed at least annually and after any changes to segmentation controls/methods to verify segmentation methods are operational, effective and isolate all out-of-scope systems from in-scope systems.

Network intrusion-detection systems and/or intrusion-prevention systems will be used to monitor all network traffic at the perimeter of the cardholder data environment as well as at critical points inside the cardholder data environment. IDS and/or IPS will be configured to alert personnel of

suspected compromises. All intrusion-detection and prevention engines, baselines and signatures will be kept up to date.

A change-detection mechanism will be implemented inside the cardholder data environment to alert personnel to unauthorized modification of critical system files, configuration files, or content files.

The change-detection mechanism will perform critical file comparisons at least weekly.

Procedures for responding to alerts from the change-detection mechanism will be documented and implemented.

5.0 Responsibility:

The Security Officer, with Executive Management supervision, is responsible for leading compliance activities that bring ABC COMPANY into compliance with the PCI Data Security Standards and other applicable regulations.

6.0 Form(s):

Wireless Access Testing Procedure *(you will need to create)*

Wireless Access Test Log *(you will need to create)*

7.0 Definition(s):

Definitions for all policies and procedures are in the Glossary of PCI DSS Terms.

8.0 Policy History:

Initial effective date: 12/31/2014