AMBERSAIL

Penetration Testing Policy

This document is a sample penetration testing policy developed by Ambersail. It forms part of the full PCI DSS policy documentation pack that can be found at https://www.pcipolicypack.com.

Read and use this document in conjunction with sample supporting procedures in the accompanying document: *Penetration Testing Procedure - Ambersail Sample*.

This document has been released as a guide on what information to include in a Penetration Testing Policy.

Document Reference	Penetration Testing Policy - Ambersail Sample
Date	1 Jul 2018
Document Status	Draft / Sample
Version	3.2
Revision History	3.0 - 30 September 2014: Initial release for PCI DSS V3. 3.1 – 27 May 2015: Update to reflect PCI DSS v3.1 changes. 3.2 – 1 Aug 2016: Update to reflect PCI DSS v3.2 changes.

Table of Contents

1. Policy Statement

This document details **<COMPANY>'s** policy with respect to penetration testing the cardholder data environment.

This document, supported by Penetration Testing Procedure constitutes <COMPANY>'s penetration Testing methodology.

- This document should be viewed in conjunction with **<COMPANY>'s** top level security policy: P01 – Information Security Policy.

2. Review and Update of the Policy Statement

The Policy Statement and associated company Policies are reviewed at least annually by **<COMPANY>'s [RESPONSIBLE TEAM]** to ensure:

- The business meets its compliance obligations to the Payment Card Industry Data Security Standard (the PCI DSS).
- Application and network components supporting the Cardholder Data Environment are periodically reviewed to identify any security weaknesses that might adversely affect business operations.
- **<COMPANY>** maintains its relevance to the business' current and planned payment card processing operations.

The **<COMPANY>'s [RESPONSIBLE TEAM]** will undertake the technical review of this policy statement and associated company Policies and Procedures.

3. Purpose

This document identifies how **<COMPANY>** performs penetration testing against its cardholder data environment to identify security weaknesses.

Penetration Testing supports **<COMPANY>'s** security best practice by confirming the controls protecting the storage, processing or transmission of Cardholder Data are effective and keep pace with i) changes to both the Cardholder Data Environment and ii) newly identified security vulnerabilities.

The frequency and nature of penetration testing meets with PCI DSS testing controls detailed in section 11.3 of the PCI DSS.

4. Scope

This document identifies the targets and testing tasks required for **<COMPANY>** to complete penetration testing to meet PCI DSS requirements**.**

The policy and supporting procedures contain the following considerations:

- Purpose of penetration testing. Overall objectives.
- Industry standards employed during penetration testing.
- Definition of targets for penetration testing.
- Staff and third parties used in the testing process.
- Frequency of penetration testing.
- Dissemination, processing and follow up of test results.

5. Policy

5.1. General Approach to Testing

Penetration testing is a key tool that is used to identify threats to the Cardholder Data Environment. To ensure that test techniques and tools meet an acceptable level of assessment, the following standards are used to define an acceptable level of testing:

- NIST Technical Guide to IS Testing and Assessment (Special Publication 800-115). Referenced at http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf .
- Application vulnerabilities as detailed in Open Web Application Security Project (OWASP). Specific reference to attack references found at: https://www.owasp.org/index.php/Category:Attack .

5.2. Overall responsibility

The person with overall responsibility for Penetration Testing at **<COMPANY>** is **<ROLE NAME>.**

Responsibilities will include:

- Selection of testers.
- Scheduling tests.
- Identifying test targets.
- Primary point of contact during test exercises.
- Receipt and dissemination of test results and reports.
- Scheduling re-tests as required.

5.3. Testing Coverage

<COMPANY> has two categories of penetration testing.

Internal Testing. To assess the security of the internal network and the internal interfaces to the Cardholder Data Environment. This will also include assessing any segmentation configuration that supports the reduction of scope of the Cardholder Data Environment.

Testing performed from within **<COMPANY>'s** internal network. Testing to be performed against the internal Cardholder Data Environment network boundary and also inside the Cardholder Data Environment.

Internal targets are detailed in Penetration Testing-Procedure & F21 - Penetration Test Targets.

External Testing. To assess the security of the external (Internet) interfaces to the Cardholder Data Environment.

Testing performed against the external facing interfaces into the Cardholder Data Environment. All tests to be performed from the public Internet to determine whether **<COMPANY>'s** external protection mechanisms are secure.

External targets are detailed in Penetration Testing-Procedure & F21 - Penetration Test Targets.

5.4. Extent of Testing

All network and application components that are contained in or are directly connected to the Cardholder Data Environment will be tested.

A complete list of internal and external targets are detailed in F21 - Penetration Test Targets.

Testing will consist of the following types / categories of testing:

- Network Testing. Specific network tests are detailed in Penetration Testing-Procedure.
- Application Testing. Specific application tests are detailed in Penetration Testing-Procedure.
- Wireless Testing. Specific wireless tests are detailed in Penetration Testing-Procedure.

5.5. Frequency of Testing

The Cardholder Data Environment must be Penetration Tested at least annually. This penetration test will consist of all components as listed in 5.3.

Service Provider Exception

As a Service Provider, From January 31st 2018, **<COMPANY>** must perform CDE segmentation penetration testing at least every six months. Segmentation testing is detailed in Penetration Testing-Procedure.

The date for penetration testing and the associated preparation and execution tasks are detailed in Network Testing. Specific network tests are detailed in Penetration Testing-Procedure.

New applications, networks or significant changes to existing Cardholder Data Environment components must undergo penetration testing at the time of the change being promoted to the 'live' or Production environment. In these cases testing of all new or changed components will be performed in:

- A Pre-production test environment that accurately reflects the existing live Cardholder Data Environment.
- On go-live in the production Cardholder Data Environment. In these cases, testing must be completed and all high level vulnerabilities fixed by [STATE ELAPSED TIME].

A significant change is considered to be a change that impacts the storage, processing or transmission of Cardholder Data in any way. **<COMPANY>** recognises that this could be:

- A new system component is introduced to the Cardholder Data Environment. For example a new server or servers.
- A new subnetwork that is directly connected to the Cardholder Data Environment.
- Major release changes to applications or operating systems that support the Cardholder Data Environment.

5.6. Testers

Penetration Testing is performed by [STATE WHO/WHICH ORGANISATION].

If an external Company

<EXTERNAL COMPANY> performs all penetration testing against the Cardholder Data Environment. The organisation has the following security testing credentials:

- List Credentials

If an internal Team

<TEAM NAME / INDIVIDUAL NAME> performs all penetration testing against the Cardholder Data Environment. The tester has the following security testing credentials:

- List Credentials (experience / qualifications).

The tester has been confirmed as being independent from the development and implementation team as follows:

- State how independent (different team / sub organisation / security contractor).

5.7. Review and Processing of Results

All penetration test results will be detailed in a comprehensive report. The results will be rated, clearly showing all high, medium and low severity vulnerabilities.

All high level vulnerabilities identified during test exercises will be immediately communicated to **<CUSTOMER>**.

<Responsible Person> will communicate all penetration test report results to the following teams.

- <List of recipients>.

All high level vulnerabilities identified during testing will be addressed as soon as possible. Once the vulnerability has been fixed a further retest will be commissioned within **<TIME>** to confirm the fix has been successful.

Further re-tests will be commissioned until any high vulnerabilities are confirmed as fixed.

Penetration Test reports will be held **<STATE WHERE>** for a period of **<STATE PERIOD>.** Results will be held under the control **<STATE WHO>.**

An annual review, performed on <DATE> will review all potential and identified threats to the Cardholder Data Environment. Penetration Test results will support this review, along with ASV scanning results, systems patching results, hardware and software vendor communications and general IT security industry updates.

6. Glossary and References

6.1. Glossary

See document P99 - Glossary

6.2. References

- P01 - Information Security Policy
- - Penetration Testing Procedure
- F21 - Penetration Test Targets