PB&J Restaurants

Credit Card Security Policies

Version 1.0 - August 20th, 2014

CONFIDENTIAL INFORMATION

Revision History

Changes	Approving Manager	Date
Initial Publication	Jacob Schnoebelen	08/20/2014

Introduction and Scope

Introduction

This document explains Restaurants' credit card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. PB&J Restaurants management is committed to these security policies to protect information utilized by PB&J Restaurants in attaining its business goals. All employees are required to adhere to the policies described within this document.

Scope of Compliance

The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, PB&J Restaurants' cardholder dataflow includes only paper media. Electronic storage of cardholder data is not conducted or permitted. Due to the limited nature of the in-scope environment, this document is intended to meet the PCI requirements as defined in Self-Assessment Questionnaire (SAQ) C, ver. 1.2, October, 2008. Should PB&J Restaurants implement additional acceptance channels, begin storing, processing, or transmitting cardholder data in electronic format, or otherwise become ineligible to validate compliance under SAQ C, it will be the responsibility of PB&J Restaurants to determine the appropriate compliance criteria and implement additional policies and controls as needed.

Requirement 1: Build and Maintain a Secure Network

Firewall Configuration

Firewalls must restrict connections between untrusted networks and any system in the cardholder data environment. An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage. (PCI Requirement 1.2)

Firewalls must prohibit direct public access between the Internet and any system component in the cardholder data environment. (PCI requirement 1.3)

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

Vendor Defaults

Vendor-supplied defaults must always be changed before install a system on the network. Examples of vendor-defaults include passwords, SNMP community strings, and elimination of unnecessary accounts. (PCI Requirement 2.1)

Defaults for wireless systems must be changed before implementation. Wireless environment defaults include, but are not limited to, default encryption keys, passwords and SNMP community strings. (PCI Requirement 2.1.1)

Non-Console Administrative Access

Credentials for non-console administrative access must be encrypted using technologies such as SSH, VPN, or SSL/TLS. (PCI Requirement 2.3)

Requirement 3: Protect Stored Cardholder Data

Prohibited Data

Sensitive authorization data will be retained only until completion of the authorization of a transaction. Storage of sensitive authorization data post-authorization is forbidden. Specifically, sensitive authorization data includes the following:

- The full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. (PCI requirement 3.2.1)
- The card verification code or value (three- or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions. (PCI requirement 3.2.2)
- The personal identification number (PIN) or the encrypted PIN block. (PCI requirement 3.2.3)

Displaying PAN

PB&J Restaurants will mask the display of PANs (primary account numbers), and limit viewing of PANs to only those employees and other parties with a legitimate need. A properly masked number will show only the first six and the last four digits of the PAN. (PCI requirement 3.3)

Requirement 4: Encrypt Transmission of Cardholder Data across Open, Public Networks

Transmission of Cardholder Data

Cardholder data sent across open, public networks must be protected through the use of strong cryptography or security protocols (e.g., IPSEC, SSLTLS). (PCI Requirement 4.1)

Sending unencrypted PANs by end-user messaging technologies is prohibited. Examples of end-user technologies include email, instant messaging and chat. (PCI requirement 4.2)

Requirement 5: use and Regularly Update Anti-Virus Software or Programs

Anti-Virus

All systems, particularly personal computers and servers commonly affected by viruses, must have installed an anti-virus program which is capable of detecting, removing, and protecting against all know types of malicious software. (PCI Requirement 5.1, 5.1.1)

All anti-virus programs must be kept current, be actively running, and capable of generating audit logs. (PCI Requirement 5.2)

Requirement 6: Develop and Maintain Secure Systems and Applications

Security Patches

All critical security patches must be installed with one month of release. (PCI Requirement 6.1)

Requirement 7: Restrict Access to Cardholder Data by Business Need to Know

Limit Access to Cardholder Data

Access to PB&J Restaurants' cardholder data is limited to only those individuals whose job requires such access. (PCI requirement 7.1)

Access limitations must include the following:

Restriction of access rights to cardholder data to the least access needed to perform job responsibilities.

Access to cardholder data is based on an individual's job classification and function.

Access to cardholder data will be granted only after completing an authorization request form. This form must be signed by management.

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Vendor Accounts

All accounts used by vendors for remote maintenance shall be enabled only during the time period needed. At all other times these accounts must be disabled. (PCI Requirement 8.5.6)

Requirement 9: Restrict Physical Access to Cardholder Data

Physically secure all Paper Containing Cardholder Data

Hard copy materials containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:

- Printed reports containing cardholder data are to be physically retained, stored or archived only within secure PB&J Restaurants office environments, and only for the minimum time deemed necessary for their use. (PCI requirement 9.6)
- All hardcopy media containing cardholder data must be stored in a secure and locked container (e.g. locker, cabinet, desk, storage bin). (PCI requirement 9.6)
- Hardcopy material containing cardholder data should never be stored in unlocked or insecure containers or open workspaces. (PCI requirement 9.6)
- All hardcopy material containing cardholder data must be easily distinguishable through labeling or other methods. (PCI requirement 9.7.1)
- All confidential or sensitive hardcopy material must be sent or delivered by a secured courier or other delivery methods that can be accurately tracked. (PCI requirement 9.7.2)
- At no time is printed material containing cardholder data to be removed from any PB&J Restaurants data center or computer room without prior authorization from management. (PCI requirement 9.8)
- Custodians of hardcopy media containing cardholder data must perform an inventory of the media at least annually. Results of inventories shall be recorded in an inventory log. (PCI requirement 9.9)

Destruction of Data

All media containing cardholder data must be destroyed when no longer needed for business or legal reasons. (PCI requirement 9.10)

Hardcopy media must be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed. (PCI requirement 9.10.1)

Requirement 11: Regularly Test Security Systems and Processes

Testing for Unauthorized Wireless Access Points

At least quarterly, PB&J Restaurants will perform testing to ensure there are no unauthorized wireless access points present in the cardholder environment. (PCI Requirement 11.1)

Vulnerability Scanning

At least quarterly, and after any significant changes in the network, PB&J Restaurants will perform vulnerability scanning on all in-scope systems. (PCI Requirement 11.2)

Vulnerability scanning shall consist of external and internal scans. External scans must be performed on any public-facing devices, and conducted by an Approved Scan Vendor qualified by the PCI Security Standards

Council. Scan conducted after network changes may be performed by internal staff. Internal scans must be performed on all in-scope systems using an internally-approved scanning product. (PCI Requirement 11.2)

Requirement 12: Maintain a Policy that Addresses Information Security for Employees and Contractors

Security Policy

PB&J Restaurants shall maintain a security policy that addresses how the company will protect cardholder data. This policy must be reviewed at least annually, and must be updated as needed to reflect changes to business objectives or the risk environment. (PCI requirement 12.1.1, 12.1.3)

Employees shall not use or otherwise employ employee-facing technologies to store, process or otherwise handle cardholder data. Employee-facing technologies include remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), email, and internet usage. (PCI requirement 12.3)

The policies and procedures delineated in this document will apply to all employees and contractors involved in the processing, or other handling of cardholder data. (PCI requirement 12.4)

Incident Response Policy

The I.T Director shall establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. (PCI requirement 12.5.3)

Incident Identification

Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents that an employee might recognize in their day to day activities include, but are not limited to,

- Theft, damage, or unauthorized access (e.g., papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry)
- Fraud – Inaccurate information within databases, logs, files or paper records

Reporting an Incident

The I.T Director should be notified immediately of any suspected or real security incidents involving cardholder data:

- Contact the I.T Director to report any suspected or actual incidents. The Internal Audit's phone number should be well known to all employees and should page someone during non-business hours.
- No one should communicate with anyone outside of their supervisor(s) and owners about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the I.T Director.
- Document any information you know while waiting for the I.T Director to respond to the incident. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.

Incident Response

Responses can include or proceed through the following stages: identification, severity classification, containment, eradication, recovery and root cause analysis resulting in improvement of security controls.

Contain, Eradicate, Recover and perform Root Cause Analysis

1. Notify applicable card associations.

   Visa

   Provide the compromised Visa accounts to Visa Fraud Control Group within ten (10) business days. For assistance, contact 1-(650)-432-2978. Account numbers must be securely sent to Visa as instructed by the Visa Fraud Control Group. It is critical that all potentially compromised accounts are provided. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information. See Visa's "What to do if compromised" documentation for additional activities that must be performed. That documentation can be found at http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_what_to_do_if_compromised.pdf

   MasterCard

   Contact your merchant bank for specific details on what to do following a compromise. Details on the merchant bank (aka. the acquirer) can be found in the Merchant Manual at http://www.mastercard.com/us/wce/PDF/12999_MERC-Entire_Manual.pdf. Your merchant bank will assist when you call MasterCard at 1-(636)-722-4100.

   Discover Card

   Contact your relationship manager or call the support line at 1-(800)-347-3083 for further guidance.

2. Alert all necessary parties. Be sure to notify:
   a. Merchant bank
   b. Local FBI Office
   c. U.S. Secret Service (if Visa payment data is compromised)
   d. Local authorities (if appropriate)
3. Perform an analysis of legal requirements for reporting compromises in every state where clients were affected. The following source of information must be used: http://www.ncsl.org/programs/lis/cip/priv/breach.htm
4. Collect and protect information associated with the intrusion. In the event that forensic investigation is required the I.T Director will work with legal and management to identify appropriate forensic specialists.
5. Eliminate the intruder's means of access and any related vulnerabilities.
6. Research potential risks related to or damage caused by intrusion method used.

Root Cause Analysis and Lessons Learned

Not more than one week following the incident, members of the Corporate Office and all affected parties will meet to review the results of any investigation to determine the root cause of the compromise and evaluate the effectiveness of the *Incident Response Plan*. Review other security controls to determine their appropriateness for the current risks. Any identified areas in which the plan, policy or security control can be made more effective or efficient, must be updated accordingly.

Security Awareness

PB&J Restaurants shall implement and maintain an security awareness program with the intent of ensuring all employees that process, store, or are otherwise involved in handling cardholder data are aware of the importance of cardholder data security. (PCI requirement 12.6)

PB&J Restaurants will ensure employees receive security awareness training upon hire and at least annually. The security awareness program must provide multiple methods of educating employees, including posters, letters, memos, web-based training, meetings, or promotions. (PCI requirement 12.6.1)

Service Providers

PB&J Restaurants will implement policies and procedures to manage service providers. (PCI requirement 12.8) This process must include the following:

- Maintain a list of service providers (PCI requirement 12.8.1)
- Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of the cardholder data the service providers possess (PCI requirement 12.8.2)
- Implement a process to perform proper due diligence prior to engaging a service provider (PCI requirement 12.8.3)
- Monitor service providers' PCI DSS compliance status (PCI requirement 12.8.4)

This page is intentionally blank to indicate the end of this document.