Date:	
Audited By:	
Campus Department:	
Responsible Person:	
Signed & Understood:	
Date Signed:	

SJSU Bursar's Office: Review for Main Office and Satellite Operations

PCI Compliance Self Assessment Questions

Protecting stored data

1.1. Is sensitive data securely disposed of when no longer needed?

1.2. Are all but the last four digits of the account number masked when displaying cardholder data?

1.3. Are account numbers sanitized before being logged in the audit log?

1.4. Is it prohibited to store the full contents of any track from the magnetic stripe (on the back of the card, in a chip, etc.) in the database, log files, or point of sale products?

1.5. Is it understood that credit card information (whole credit card numbers) should never be emailed on open, public networks?

1.6. Is it prohibited to store the care-validation code (3 digit value printed on the signature panel of a card) in the database, log files, or point of sale products?

1.7. Are account numbers (in databases, logs, files, back up media, etc) stored securely - for example, by means of encryption or truncation?

Protecting ID's

2.1. When an employee leaves the company, are that employee's user accounts and passwords immediately revoked?

2.2. Are all user accounts reviewed on a regular basis to ensure that malicious, out-of-date, or unknown accounts do not exist?

Restrict physical access to cardholder data

3.1. Is all cardholder data printed on paper or received by fax protected against unauthorized access and seen only by those on a "need to know" basis? For example, those processing the transaction, those accounting for the transaction, or those processing a refund for a credit card transaction.

3.2. Are procedures in place to handle secure distribution and disposal of back up media and other media containing sensitive cardholder data?

3.3. Is cardholder data deleted or destroyed before it is physically disposed (for example, by shredding papers or degaussing back up media)?

Track and monitor all access to network resources and cardholder data

4.1. Is all access to cardholder data, including root/administration access, logged?

Maintain a policy that addresses information security

5.1. Are information security policies reviewed at least once a year and updated as needed?

5.2. Have the roles and responsibilities for information security been clearly defined within the company?

5.3. Are employees required to sign an agreement verifying they have read and understood the security policies & procedures?

5.4. Is a background investigation (such as a credit & criminal record check, within the limits of local law) performed on all employees with access to account numbers?

5.5. Are all third parties with access to sensitive cardholder data contractually obligated to comply with card association security standards? For more info: https://www.pcisecuritystandards.org

5.6. Are security incidents reported to the person responsible for security investigation?

5.7. Is there an incident response team ready to be deployed in case of a cardholder data compromise?