Galleon Centre Merchant Credit Card Policy for Processors

Policy Statement

The Galleon Centre requires all departments that process, store or transmit credit card data remain in compliance with the Payment Card Industry Data Security Standard (PCI DSS). The purpose of the Merchant Credit Card Policy is to protect our customers' credit card data, to uphold the Centre's reputation, to reduce the financial costs associated with a breach of credit card information and to outline best practices for all aspect of credit card transactions.

Background

Every merchant who handles credit card data is responsible for safeguarding that information and can be held liable for security compromises.
The project objective is to review all credit card merchant accounts, identify all the systems, applications and devices that process, store or transmit cardholder data.

Scope of Policy

Departments that accept credit card payments and retain sensitive cardholder data in paper or electronic format.

Who Should Read This Policy

- **Merchant Credit Card Policy – for Processors (how to handle credit card information)**

Any persons with the responsibilities of processing, storing or transmitting credit card data.

Security, Protection, Vulnerability, Access Control and Test Processes.

Requirement 1: Install and maintain a firewall configuration to protect cardholder data
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
Requirement 3: Protect stored cardholder data
Requirement 4: Encrypt transmission of cardholder data across open, public networks
Requirement 5: Use and regularly update anti-virus software
Requirement 6: Develop and maintain secure systems and applications
Requirement 7: Restrict access to cardholder data by business need-to-know
Requirement 8: Assign a unique ID to each person with computer access
Requirement 9: Restrict physical access to cardholder data
Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes
Requirement 12: Maintain a policy that addresses information security

Compliance Certification Process

Reconciliation

The owner of the merchant account will receive a weekly/monthly statement of activity from the credit card processor. This statement must be reconciled to expected income.

Local Policies

Retention

PCI DSS recommends keeping to a minimum the credit card information that is retained. Local policy should make it a practice not to retain sensitive cardholder data. Limit your storage amount and retention time to that which is required for legal or regulatory purposes.

- Electronic – The Centre's policy is that no credit card data will be stored on laptops and/or PC's.
- Paper – Files with credit card information should be stored in a secure area on site for 7 years. Any paper containing credit card data must be shredded before disposal.

Chargeback

The payment processor will notify a merchant of a disputed charge. The merchant is responsible to provide the bank with written proof that the transaction was authorised by the customer.

Refunds

When an item or service is purchased using a credit card, and a refund is necessary, the refund must be credited only to the same account from which the purchase was made. In addition, under no circumstances is it permissible to issue cash refund. Refunds are only processed using two-factor authentication e.g. card processing machine required along with customer card/number and also Supervisor card.

Responsibilities

1) General Responsibilities for Processors:

You should NOT do the following:

1. Do not leave card processing machine in an unsecured area.
2. Do not transmit cardholder's credit card data by e-mail or fax
3. Do not store credit card data for repeat customers on paper in an unsecured area.
4. Do not store PIN or CVV2/CVC2/CID number
5. Do not electronically store on the Centres computer file or server any unencrypted credit card data
6. Do not electronically store any credit card data on laptop or PC's
7. Do not share user IDs for systems access
8. Never acquire or disclose any cardholder's data without the cardholder's consent

You should DO the following:

1. Ensure machine is switched off and signed off when not in use.
2. Store all physical documents containing credit card data in a locked drawer, locked file cabinet, or locked office
3. Maintain strict control over the internal and external distribution that contains credit card data
4. Change vendor supplied or default passwords
5. Properly dispose of any media containing credit card data
6. If you receive an unencrypted email from customer with credit card data notify the customer that they should no longer send this information via email and delete email immediately

Fraudulent Transaction Procedures

Look out for fraud warning signs

Look out for...

- **Rapid repeat visits** – A customer who returns to buy more in a short period of time may be making the most of the fact that the card has been accepted already.
- **Nervous or hurried customers** – They may be worried about being caught.
- **Cards signed in felt-tip pen** – This can be used to disguise the original signature – remember all cards should be signed in ballpoint pen.
- **Interruptions** – A customer who tries to distract you during the transaction, and who seems fully conversant with how the authorisation process works, may be trying to prevent you from noticing something suspicious.

Take extra care when a signature is needed

Nearly all cards in the UK now use chip and pin although in certain circumstances, you can accept:

- **Chip and signature cards** – You should only use a signature to verify a transaction in exceptional cases. The main ones are if the customer has a non-UK-issued card, or an impairment that means they need to sign. Your terminal will prompt you to ask for a signature. Never accept a signature just because the customer doesn't know their PIN.
- **Magnetic stripe and signature cards** – These will mostly be non-UK-issued cards from countries that have not yet upgraded to chip and PIN.

Some basic fraud checks to use when a signature is required

If you do carry out a transaction using a signature as verification, you should take extra security precautions:

- Check the cardholder's signature matches that on the back of the card.
- If possible, check that the spelling on the card is the same as the signature – fraudsters sometimes don't spell the name correctly.
- Check the title on the card matches the gender of the person presenting it.
- Check the signature strip for tampering – has another strip been placed over the top of the original one? If the word "void" appears on the strip, this could be an indication that the genuine signature has been removed and a substitute used.
- While the point-of-sale receipt is printing, check the last four digits of the card number on the receipt match those on the front of the card. If they don't contact Streamline for Authorisation.

If the Authorisation Centre asks you to retain the card

Explain politely that the card issuer has asked you to hold onto the card. Anything suspicious would be referred to the Duty Manager who in turn would notify the Police if appropriate. Never put yourself, your staff or the public at risk.

Even if the Authorisation Centre does not ask you to retain the card, you may decide that a card or a transaction is suspicious – for example, if you have identified it as counterfeit. Card thieves act fast, and will often try to use a card before the owner notices that it has gone.

Preserving evidence

Cards used fraudulently are EVIDENCE.
Treat them with care and you will make it easier for the Police to catch and prosecute the thieves.

If staff come into contact with criminals, it is far better – and less stressful – if they are prepared for the possibility and have an agreed process to follow.

- Preserve the card:
- Don't cut the card in half!
- Handle it by the edges so as to preserve fingerprints. Cut off the bottom left-hand corner (as seen from the front).
- Don't damage any other part of the card. Handle it as little as possible and place it in a plastic bag or envelope until you can give it to the Police.
- Keep the voucher or receipt:
- Keep the best copy possible.
- Don't pin or staple anything to it. Put it in the same envelope/bag as the card to give to the Police.
- Keep the video/CCTV:
- If you have a video surveillance system, keep the tape and give it to the Police.
- Keep a copy if you can.
- Note down a description of the presenter:
- Write down the details immediately while they are fresh in your memory.
- Think about the person's unique features such as their accent, scars, tattoos and body language rather than the clothes they are wearing.

Involving Police

In the event that the Police are called, they may ask for the card. You should:

- Allow the Police Officer to take it.
- Take a note of the officer's name, number and station.
- Obtain the Crime Reference Number.
- Get a receipt and keep it safely.
- Tell the Authorisation Centre.