Data Security Policy

dojo®

Document control

Version:	1.0
Date	9th June 2020
Owned by:	Dojo

Review and update policy

Dojo will review this document annually, as required by the PCI compliance process. The document may then be updated based on the results of the review.

Date	Summary of Findings & Updates	Reviewer

1. Introduction

The first step to accepting card payments is learning how to securely handle customer data so you can protect yourself and your customers from fraud.

This means following the guidelines set out by the Payment Card Industry Data Standard (PCI DSS). You'll find these guidelines in our P2PE Instruction Manual (PIM). The PIM explains how to install, operate and maintain your card machine while keeping your cardholder data safe and secure.

The Data Security Policy provides practical advice to help you follow security procedures. It also explains what to do in the event of a breach and provides training guidance you can share with your staff.

By following the guidelines in these two documents you can fully comply with the PCI P2PE standards.

We'll need your business signatory's official agreement to follow these procedures. However, PCI compliance is the responsibility of every staff member and anyone else who interacts with your card machines and cardholder data. They should all read and acknowledge the guidelines in this document, regardless of their role or the size of the business.

We will regularly review this document, along with the P2PE Instruction Manual (PIM) and let you know about any changes. The latest version can be accessed from your Dojo account and you should make sure you are following and sharing up-to-date guidance within your business.

2. Cardholder data and card machine devices

Cardholder account data should only be stored, processed or transmitted on card machines that meet the requirements of our PCI P2PE solution. This includes the customer's Primary Account Number (PAN) (the 16 digit account number) and the CVV (card verification value).

All Dojo P2PE card machines have been validated and are compliant with our PCI P2PE solution. Any receipts printed from them will mask the PAN to protect cardholder data.

Access to cardholder data should be strictly limited to those people who need it for their job. Staff members who work with card machines should be trained using the latest data security document.

If we need access to your card machine, we'll ask for your consent in advance. Always make sure you verify the identity of any Dojo staff or engineers who visit your business requesting access to your equipment.

You need to do the following:

1. Regularly check the card machine inventory held within your Dojo account – and notify us immediately if it needs updating or if you've made a change (for example, moving a device to a different location). It's your responsibility to keep us informed. Each card machine's make, model, serial number, location and status are listed within your account.

2. Check the card machines at least once a month for any evidence of tampering. Are there unexpected attachments or cables plugged into the device? Are there missing or changed security labels? Is the casing broken or differently coloured? Substitution is another possibility, so check the serial number. For reference, use the photos contained in the P2PE Inspection Manual (PIM).

3. Train staff to be alert to suspicious behaviour, such as tampering with or replacement of card machines. In particular, they should verify any anyone claiming to be a repair or maintenance operative before granting them access to the card machine. **Relevant training guidance can be found in Appendix A of this document and should be made available to all staff.**

4. Train staff to follow the reporting procedures in Section 5 if they identify any suspicious behaviour or suspect that a device has been tampered with or replaced.

5. Provide support materials at the point of sale for staff to reference (as covered by the Training guidance in Appendix A):

    a. How to verify anyone claiming to be a repair or maintenance operative before allowing them to modify or troubleshoot the device

    b. How to stop any third party from installing, replacing or returning devices without verifying their identity

    c. How to spot and report suspicious behavior related to the device

    d. How to identify and report suspected or verified device tampering or substitution to an appropriate manager.

3. Incident response

This section covers what to do if you or a staff member suspect or identify that a card machine device has been tampered with or substituted in a way that could cause a data breach.

You need to make sure that:

1. You or a staff member immediately switch off and remove any suspected or identified tampered card machine device from service. This device must not be used and should be placed in a secure location.

2. You or a staff member report the suspected or identified breach to Dojo immediately by contacting Customer Support on 0800 044 3550.

3. Staff should report and escalate to you, or another appropriate manager, any suspicious behaviour they identify relating to a card machine device.

4. Information security

Information security policies play an important role in preventing data breaches by helping to restrict sensitive information to authorised staff. Their content varies according to the complexity of your business and premises. **Appendix B contains a basic policy that you are agreeing to follow if you have no alternative policy in place.**

You need to make sure that you:

1. Annually review your Information Security Policy and update it when necessary (for example, whenever there is a change in your point of sale environment).
2. Write the policy in a way that details all staff responsibilities. You can adapt the policy in Appendix B to match your company's staff set up.
3. Distribute the Information Security policy to all staff and ensure they are aware of their responsibilities.

5. Our agreement with you

As a third party service supplier to your business, Dojo is involved in the capture, storage, processing and transmission of cardholder data on your behalf.

Because of our ongoing access to your cardholder data, we must keep it safe and secure. This means complying with PCI-DSS.

Every year, we complete a PCI-DSS assessment, carried out by an independent Qualified Security Assessor in which we attest our compliance.

You can review our Attestation of Compliance (AoC) anytime at Dojo.tech/documents.

If we suspect or identify that your cardholder data has been acquired or accessed by an unauthorised person, we will notify you as soon as possible.

Appendix A

Training guidance

This section provides guidance that can be shared with your staff so they understand how to work with card machines in a way that protects cardholder data.

1. Protecting cardholder data

Cardholder data is sensitive information that must be protected. It includes:

- The primary account number (PAN), a 16 digit number on the front of the card
- The card verification code (CVV), a 3 or 4 digit number printed on the card

Cardholder data should only be processed, transmitted and stored using card machines that have been approved and validated by the PCI P2PE solution.

When accepting a customer's card you should not write down or store any of the cardholder data, either on paper or electronically.

All Dojo card devices print receipts that mask the PAN in order to protect cardholder data from being captured.

2. Card machine inspections

Card machines should be regularly checked to ensure they've not been interfered with or replaced and that cardholder data is still protected.

2.1. Tampering

You'll need to physically inspect the device to detect any tampering. Here's what to look for:

- any unexpected attachments
- new cables plugged in to the device
- missing or changed security labels or seals
- any changes in the physical appearance of the device, such as different coloured casing or base

If any evidence of tampering is identified, you must stop using the device immediately, take it out of service and report everything to an appropriate manager or staff member.

2.2. Substitution

Regularly check the serial number on the device to ensure it matches your records, and that the device hasn't been substituted. A list of all the card machines used by your business can be found within your Dojo account.

If you identify that the machine has been substituted with another device, you must stop using it immediately, take it out of service and report everything to an appropriate manager or staff member.

2.3. Suspicious behaviour

Make sure that card machines are visible at all times. If you notice anyone acting suspiciously around the device or attempting to tamper with or substitute it, report it immediately to an appropriate manager or staff member within the business.

Examples of suspicious behaviour could involve unknown persons doing any of the following:

- attempting to remove or swap the device
- attempting to unplug or switch cables with the device
- attempting to attach something to the device
- attempting to make configuration changes to the device

3. Third Party Access

A card machine may need to be repaired, swapped or replaced if there's been a technical issue. Dojo would then authorise an inspection or return of the device and provide the following details:

- Name of the person attending
- Date and time of the person attending
- Courier service

If a third party wants access to the device, this should only be given when their identity has been verified. If this is not possible, you should take the matter up with an appropriate manager or member of staff within the business.

You must not install, replace or return devices without verifying the identity of any third party involvement.

Appendix B

Information Security Policy

1. Introduction

As a business, we handle sensitive cardholder and company data every day. It's important to safeguard information like this so we can protect cardholder privacy and meet our regulatory obligations.

This policy will outline how we'll handle sensitive data, what we'll do to secure our systems and what steps we'll take if a breach happens.

As part of this policy, we'll distribute it, along with our Training Guidance to all new staff members. We'll also send it out periodically to everyone in the company to promote awareness of our Information Security procedures.

This policy will be reviewed annually and updated whenever necessary to meet the needs of our business.

If anything in this document is unclear, you should seek guidance from an appropriate manager or from the business owner.

2. Your responsibilities

You are responsible for following and enforcing these guidelines as part of your role. So, you should promptly report any identified breach or potential violation of these guidelines to an appropriate manager or to the business owner.

3. Acceptable use and protecting business devices and data

We are committed to protecting customers, employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. This acceptable use policy has been written to ensure all devices and systems are kept and used securely.

To achieve this, all staff must:

- Regularly check card machine devices for signs of tampering or substitution (review Training Guidance 'Card Machine Inspections' for further details)
- Ensure third party credentials are checked and verified before allowing access to any card machine devices (review Training Guidance 'Third Party Access')
- Maintain appropriate credentials and authentication for the use of company devices and systems
- Take all reasonable and necessary steps to prevent unauthorised access to confidential data
- Keep all passwords secure and never share accounts
- Secure all company devices with use of a password (ensuring it is secured when leaving devices unattended)
- Take care when using portable computers/laptops to keep them secure and within your possession
- Be careful when opening email attachments from unknown sources or senders

- Immediately notify an appropriate manager if they suspect they have downloaded an attachment containing a virus

4. Access control

Access to sensitive and confidential data is strictly controlled to keep it beyond the reach of unauthorised individuals. Only those whose roles specifically require access to this information will be allowed to view it – and this requirement will be clearly defined and based on a legitimate need. No other staff members can have access.

Where cardholder data is shared with third party organisations, such as service providers, a list of these parties will be maintained. In addition, a written agreement will acknowledge that the third party is responsible for protecting sensitive and confidential information. We will also complete our due diligence on any third parties we engage – and monitor and record their PCI-DSS compliance status.

5. Incident response plan

If you identify a breach, or potential breach, of the company data or systems, you should report it to your manager right away.

The issue will be raised with the company's security officer – who may be a manager or business owner. They will then take the necessary steps to contain and resolve the issue while also informing anyone that may be affected.

If the breach has led to unauthorised access of cardholder data, the security officer will inform the following and then follow their guidance:

- Acquiring service provider
- Relevant card schemes (e.g. Visa, Mastercard, Amex, Discover)