Security POLICY (card payments)

Version Control

Version	Author	Change description	Consultation	Board approval
1.0	S brodie	First draft		

Contents

Security Policy

Processing Electronic Card payments

1. Introduction and Policy Aim

1.1. The Payment Card Industry Data Security Standard (PCI-DSS) is a worldwide information security standard, created to help organisations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise. It applies to all organisations that receive, process, store and pass cardholder information. This policy is required to ensure compliance with Point 9 and 12 of the PCI-DSS Standard.

2. Policy Statement

2.1. All card processing activities of Live Borders will comply with the PCI-DSS industry standard. No activity or technology may obstruct compliance with the PCI DSS.

3. Those Affected by the Policy

3.1. Anyone performing Live Borders duties or providing Live Borders services facilitating card payments. It applies to employees; other organisations conducting Live Borders business; contractual third parties and agents of Live Borders.

4. Roles and Responsibilities

- Live Borders employees – must understand and comply with the policy.
- Live Borders Managers and Team Leaders – must ensure their staff understand the policy and are aware of their obligation to comply with it.
- Finance manager– must ensure relevant card payment security training is carried out and that staff comply with this policy.
- IT Services – must manage IT Services and Infrastructure in accordance with the requirements of PCI DSS.

4.1. Services must comply with this policy to minimise the risk to both customers and Live Borders. Failure to comply will render Live Borders liable for fines and may also result in Credit Card providers preventing transactions from being processed.

5. Policy Compliance

5.1. This policy is mandatory for all staff. Failure to comply with this procedure may result in disciplinary or other action.

5.2. Heads of Service are responsible for ensuring that their staff are aware of the policy and that it is complied with.

5.3. If you do not understand this policy, or how it may apply to you, get advice from your manager, or from the Finance on 01896 661 166. Alternatively, email finance@liveborders.org.uk

6. Further actions to ensure compliance:

6.1. Live Borders submits an annual Self-Assessment Questionnaire (SAQ) to prove compliancy.

6.2. Live Borders will contractually require all third parties with access to cardholder data to adhere to PCI-DSS requirements. These contracts will clearly define information security responsibilities for contractors.

6.3. Ad hoc checks will take place to ensure employees are maintaining PCI-DSS security procedures.

6.4. Annual compliancy confirmation (Form X) will be sought from all staff processing electronic card payments.

7. Applying the Policy – Security Breaches

7.1. In the event of there being a security breach of data, staff must contact the Data Protection Officer and ensure that card processing is discontinued immediately.

8. Online Processing

8.1. In the first instance customers should make payment for goods and services online using the links to third party providers on the Live Borders website or app. This is the preferred method and best practice for taking payments.

8.2. On completion of a successful payment the online system being used will automatically generate an email payment confirmation to the customer.

8.3. If a customer's payment has been unsuccessful or declined, the customer in the first instance should contact their card provider. The most common reason for a declined transaction is the card provider suspecting the transaction may be fraudulent.

8.4. If a customer faces difficulty in making a payment they can email enquiries@liveborders.org.uk for assistance or phone 01896 661 166

9. Telephone Processing

9.1. Various payments can be taken over the telephone by either a Business Support Assistant agent or specific service officer.

9.2. Card details must never be written down by any member of staff for a future payment attempt. For all card details which are processed through the corporate payments system, no card details are retained by the authority.

9.3. Where card details are provided during a telephone call, these must be processed directly into the PDQ terminal at that time and must not be written down or noted anywhere.

9.4. When card details are being provided in a telephone call these must not be repeated back to the customer in such a way as to be audible to third parties.

9.5. If it is not possible to submit the card details immediately then a call back must be requested or offered.

9.6. All card processing on site or by telephone must be in compliance with the Financial Procedures.

9.7. There is no internal Live Borders access to full card details as this information is not stored within the Live Borders IT network.

10. Customer Present with a Card

10.1. When the customer is present the card should be processed through the EPOS machine according to the machine instructions.

10.2. If the transaction is successfully processed, the merchant copy should be stored securely (in compliance with Live Borders Financial Procedures) and the customer copy given to the customer, should they wish a copy.

10.3. If the transaction is declined, the customer should be advised immediately. The option of paying with a different card should be offered. The customer copy stating that the payment was declined should be given to the customer and the merchant copy should be stored securely (see Storage of Card Details).

10.4. Live Borders will not accept card details in writing either by letter or email. There is a risk that either may have been intercepted.

10.5. If card details have been received in writing the sender must be contacted by phone, email or letter and advised that the letter or email will / has been securely destroyed, response by letter or email will require the customer to call Live Borders to make payment or receive refund. Once contact is made by phone the transaction can then be carried out in the normal way.

10.6. Under no circumstances should a refund be processed to a card whose details were received either by email or letter.

11. Applying the Policy – Refunds

11.1. Corporate Electronic Payments - payments made online must be refunded to the originating card.

11.2. Refunds can only be processed back to the originating card if:

- the card is still valid and
- if the payment was made either online or via the telephone where customer information has been completed (but not automated payment line or Kiosk card transactions).

11.3. The refund must be approved by the responsible Budget Holder.

11.4. The corporate system is then accessed, and the refund is processed back to the source card from which the original transaction was authorised where possible. It is possible to process part refunds where necessary but the refund cannot exceed the original amount.

12. Applying the Policy – Electronic Transfer of Data

12.1. It is strictly prohibited to transfer card data electronically both internally or externally to Live Borders This includes the use of end user messaging technologies.

13. Applying the Policy - Point of Sale (EPoS) Card Devices

13.1. All devices in use must comply with PCI standards.

13.2. All devices are included in the inventory held by Live Borders which contains key data identified by the standard.

13.3. Devices must be periodically inspected to detect tampering or substitution.

13.4. Staff using such devices must be trained to be aware of attempted tampering or replacement of devices.

13.5. Services using such devices must take ownership of their use and adhere to the requirements listed above.

14. Implications of breach of policy – Storage of Card Details

14.1. Storage of card details on any media in any format (e.g. email, Access databases, Excel spreadsheets is not permitted and breaches the Security Standard Regulations. Media is any computer, USB drive, mobile phone etc. **If this occurs the result could be large monetary fines from credit card providers.**

15. Related Policies and Procedures

- Data protection Policy
- Financial procedures

16. Review

16.1. Reviewed annually to comply with PCI-DSS security requirements.