University of Bristol

PCI DSS training for staff who take credit or debit card payments

PCI DSS = Payment Card Industry Data Security Standards, a worldwide standard to help businesses process card payments securely and reduce card fraud.

How might a breach occur?

Swapping a point of sale (POS) terminal for a compromised one, tampering with a POS terminal, Stolen POS terminal, installing malware (fake technician or service engineer), skimming or key logging hardware, new compromised terminals delivered with instructions to return original terminal

Actions

POS

- All devices must be securely stored when not in use
- All devices must be checked regularly for tampering or substitution
- Any suspicion of tampering must be reported in line with the Incident response Procedure (below)
- Default passwords must be changed and shared with relevant staff only
- Change passwords when staff leave and maintain records of who has access
- Terminals must be type approved by the Income Office who will keep and maintain a record of all models, serial numbers, security features and location
- New or replacement terminals must be delivered to the Income Office in normal circumstances. Secure arrangements must be made when emergency replacement terminals are delivered.
- Spot checks will be carried out by Finance Services
- Terminals and Merchant IDs must be surrendered when no longer required
- Refunds must only be made only to the original payment card
- POS terminals should not be taken abroad or used at any location other than the merchant ID number they are linked to.

Handling Cardholder Data – Cardholder Present

- Cards must remain visible to the cardholder at all times
- Merchant copies of receipts must be stored securely and destroyed within 12 months
- Ensure cameras positions do not record cardholder data e.g customers putting PINs into terminals.

Handling Cardholder Data – Cardholder Not Present

- Do not request cardholder details by email, instant message or SMS
- Consider who can hear if you need to repeat the card details back to the cardholder
- If a cardholder emails details, do not reply and contact IT services to ensure it is securely deleted.
- Do not record telephone calls or use Voice Over Internet Protocol (VOIP)
- Never write down the card details when receiving them over the phone. If in exceptional circumstances you have to, make sure it is stored securely and destroyed after authorisation.
- Do not store cardholder data on hard drives, shared storage, cloud storage or any other removable media.
- Any stored cardholder data should be reported to dg-carddatabreach@bristol.ac.uk immediately on discovery.

Last Updated: July 2020, *Angela Nansera, Income Office Manager*

Incident Response Plan: **Responding to a suspected breach**

- DO NOT SHUT DOWN the suspected POS terminal
- IMMEDIATELY DISCONNECT the network cable from the back of the machine or base to contain and limit the exposure.
- DOCUMENT all steps taken. Include the date, time, location(s), person/people involved and action taken for each step.
- LABEL the machine 'Do not touch unless directed by the PCI Incident
- REPORT the incident to the PCI Incident Response Team

Incident Response Plan: **Reporting a breach 08.00 – 17.00 Monday – Friday**

A breach might be discovered by our acquirer or a member of staff.
Once the Incident Response Procedure has been completed, immediately contact a member of the PCI DSS Incident Response Team below (priority order):

1. Alex Baylies – Information Security Officer, phone: (0117) 45 50297
2. Shirlene Adam - Director of Financial Operations, phone: (0117) 42 84718
3. Angela Nansera – Income Office Manager, phone: (0117) 928 7908
4. Jason Smerdon – Group Finance Director, phone: (0117) 42 82585

All of the above are members of an Incident Response Team and they will immediately invoke our Incident Response Plan.

Staff should inform their Supervisor, MID Manager and/or Deputy MID Manager as soon as possible after detecting the breach.

Incident Response Plan: **Reporting a breach out of business hours**

1. Once the Incident Response Procedure has been completed immediately email dg-carddatabreach@bristol.ac.uk with the details of the breach and who can be contacted for further information.
2. Please use 'BREACH' in the heading of the email and remember not to include any cardholder data.
3. Staff should inform their Supervisor, MID Manager and/or Deputy MID Manager as soon as possible after detecting the breach.

Please don't hesitate to contact your MID Manager or the PCI DSS team (dg-carddatabreach@bristol.ac.uk) if you have any questions.

Last Updated: July 2020, *Angela Nansera, Income Office Manager*