Debit/Credit Card Use and Storage Security Guidance

Introduction

This document outlines the credit card security requirements as per the Payment Card Industry Data Security Standards (PCI DSS). The standards apply to all organisations who receive, process, store and pass Credit/debit card information and were created to prevent card fraud through increased controls around data and its exposure to compromise.

This policy document covers all aspects of security surrounding the use of credit/debit card machines and confidential University information and must be distributed to all employees and adhered to within each University outlet that uses PDQs/Card terminals.

These employees must read this document in its entirety and retain it for information, Staff are required to sign the form at appendix 1 confirming they have read and understood this policy fully and return it to the Treasury & Transactions Manager, Finance Services Sighthill 6.B.32.

This document will be reviewed and updated by Finance on an annual basis or when required to include any newly developed or amended credit/debit card security standards into the policy. (This policy can be found on the PCI DSS SharePoint Site)

Ethics and Acceptable Use Policies

All University employees are required to conduct business in accordance with all relevant University polices, applicable laws, regulations and contractual obligations.

It is the responsibility of each employee to co-operate fully with credit/debit card information security standards and regulations set out by Edinburgh Napier University.

It is also the responsibility of each employee to report inappropriate activity or breaches in the use, storage, security of debit/credit card details and unlawful conduct by another employee to a supervisor and escalated to Finance.

Consumer confidence is of paramount importance to our business and with this in mind the security and protection of sensitive information is crucial. It is imperative that employees understand the importance of safeguarding such sensitive information.

Examples of personal data include;

- Bank account details
- Credit card details
- name,
- address,
- telephone numbers etc

Plus other information that is not readily available to the public (clients, financial information, employee information, schedules, technology etc.).

Disciplinary Action

Non-compliance with the PCI-DSS standards can result in substantial fines from its merchant bankers and the facility to take debit/credit payments whether by Cardholder present, card holder not present, on-line payments via EPAY or the STORE could be rescinded resulting in significant damage to the University's reputation and standing.

Violation of the standards, policies and procedures presented in this document by any University employee may result in disciplinary action.

Protect Stored Data

All sensitive information must be stored securely and disposed of in a secure and irrecoverable manner by crisscross shredding.

All cardholder data stored and handled by the University and its employees must be securely protected against unauthorised use at all times.

Credit card information – handling specifics.

All media (e.g. paper, floppy disks, backup tape, computer hard drive, etc.) that contains cardholder information must be discarded securely and irreversibly by means such as shredding, demagnetizing, disassembly, etc. when it is no longer needed.

Don'ts

It is strictly prohibited to store:

- The contents of the credit card magnetic strip (track data) on any media.
- The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the card) on any media whatsoever
- All digits of the credit cards Primary Account Number (PAN) on any media. All digits but the last 4 numbers of the credit card account number must be truncated/ concealed or masked e.g. XXXX or **** or swiped over with black permanent marker (both sides of paper)
- Cardholder information on PC's or any other electronic media, Cardholder information is defined as;-
    - Card account number
    - Expiry date
    - Cardholder name (in conjunction with above)
- Do not write PAN's/card numbers/security codes when taking card payments over the phone.
- Do not send or transmit card details by Email or in the internal /external post (please see section of protection of data in transit below for further info)
- Do not under any circumstance leave card details on desks or in an unsecured office environment.

Do's

- All sensitive information must be stored securely in a secure environment with controlled access e.g locked filling cabinet, cupboard, cabinet or safe
- Ensure access to card storage areas is restricted to staff whose role includes taking and /or processing card payments and access to these areas must be limited to those who take and process payments.
- Data should not be stored for longer than 2 months, and data no longer required has to be shredded using a crisscross shredder.

- The card security code and the rest of card data information must be stored separately
- The PDQ machine must be checked weekly for tampering and to ensure the terminal number is correct.(the terminal number can be found underneath the terminal handset)
- Ensure that policies and procedures within each area are documented and accessible.
- Conduct internal operational audits to ensure compliance with procedures
- Develop an escalation plan to notify Finance/Information Services should a breach occur.

Protection of Data in Transit (of campus e.g. Graduation ceremonies, accommodation key collection)

Sensitive data should never be transported electronically for out of office environments where card payments are taken. The following procedure must be followed to ensure that data is secure at all times,

Do's

- The PDQ machine being used must be checked to ensure the terminal number is correct for reference the terminal number can be found underneath the terminal handset)
- Ensure that any credit card receipts are securely stored while at the venue
- Once the cashing up has been completed, all credit card receipts should be secured in the blue plastic security pouch (provided by Cash Services)
- A numbered security tag must be attached and the number recorded on the paperwork (bank Giro credit tear off slip (please see instructions from Cash Services)
- At Graduation hand the blue security bags containing credit cards and one containing cash to reception staff at the Usher Hall
- Edinburgh Napier University security staff will uplift credit card details from Usher hall
- Ensure that all staff handling card payments are authorised to do so and have read and understand the procedures in keeping all data and terminal secure at all times.

Don'ts

- Do not leave the PDQ (card terminals) unattended at any time
- Do not leave credit card receipts unsecured at any time

Protection of data at Face to Face Checks

Security of card data is paramount, to enable compliance with PCI DSS standards, additional processes must be applied to specific PC's, which students are directed to at face to face finance checks during fresher's week.

- Allocated PC's are to be identified prior to face to face sessions
- Access to the PC's is restricted to students for use in the face to face sessions only.
- The PC's are secured and locked down so they can only be booted up by authorised staff
- Passwords and user ID's are required to be used by authorised staff to access Pc's
- Access is strictly limited to the University EPAY page only
- Designated PC's are to be checked regularly by authorised finance staff to ensure that PCs are secure at all times.

Suspected/Real breach of data compromise incident

All employees who handled debit/credit card transactions have responsibility in detecting security breaches and assisting in the incident response procedures within their particular operational areas. Some examples of security issues that may be encountered in day to day activities may include, but not limited to:

- Theft, damage, or unauthorised access, (e.g. papers missing from desks, unauthorised access to secure data storage, broken locks etc.)
- Fraud- Inaccurate information e.g. on databases, files, paper records

Incident Response Plan/Security

The Finance office will establish, document and post guidelines onto the PCIDSS SharePoint site with security response guidelines to ensure timely and effective handling of suspected or real data security breaches

In the event of a compromise of sensitive data, the Incident Response Officer (ie the Treasury & Transactions Manager or Head of Financial Accounting) will oversee the execution of the incidence response plan.

No person should communicate with anyone other than their Line Manager and the Incident Response Officer any details or generalities surrounding any suspected or actual incidents. You should document any information known or thought to relate to the incident including date, time and nature of incident. Any information provided will be critical to ensure response in a timely manner.

Incidence Response Plan

If a compromise is suspected, the Incident Response Officer (normally the Treasury & Transactions Manager k.parks-smith@napier.ac.uk if the Treasury & Transactions Manager is unavailable contact the head of Financial Accounting c.macdonald@napier.ac.uk

The Incident Response Officer will

- Alert the Network Services and Security Manager
- Conduct an initial investigation of the suspected compromise
- If a compromise of breach of information is confirmed will alert Senior Management and authorised University personnel
- Inform parties that may be affected by the compromise

If the compromise involves card account numbers the Incident Response Officer will

- Contact Network Services and Security Manager to contain and limit the exposure by shutting down any processes or systems affected by the compromise
- Alert necessary parties (Merchant bank, Visa Fraud Control, Mastercard via Merchants Bank, the Police)
- Provide compromised or potentially compromised card numbers/details to Merchant Bank/Visa Fraud Control within 24 hours
- For further information see
    - ‘Account Data Compromise Master’ (PCIDSS SharePoint Site or
    - PCIDSS page on Treasury and Transactions section on staff Intranet).

Incident Analysis

After 7-10 days following the data breach and implantation of the Response Plan, the Incident Response Officer and all affected parties will meet to review;

- Results of any investigation
- Determine root cause of breach/compromise
- Evaluate effectiveness of plan
- Review other security controls to determine appropriateness of current risks
- Identify areas where procedures can be improved, and/or made more effective or efficient.
- Agree policies and procedures to be updated