SALISBURY
CITY COUNCIL

Payment Card Industry Data Security Standard Policy

Policy Number	Version	Owner	Doc No.	PDF No.	Date Published	Review Due	Review Team
FP004	3	RFO	87166	87167	29.04.21	2022	Finance
FP003	3	RFO	72308	72379	01.09.19	01.09.20	Finance
FP003	2	RFO	57261	57546	05.09.16	01.09.19	Finance
FP003	1	RFO	45110	47215	01.09.14	01.09.15	Finance

Distribution

Internal: All SCC Staff

External: Website/Councillors/Partners

1. Introduction

1.1. As an organisation which processes card-holder data, the council is obliged to comply with the Payment Card Industry Data Security Standard (PCI/DSS). This standard governs the security of information related to debit and credit cards.

1.2. Requirement 12 of the PCI DSS holds that an organisation must maintain a policy that addresses information security for all personnel. This requirement includes the statement that: “To comply with the PCI DSS, organisations must establish, publish, maintain and disseminate a security policy, which must be reviewed at least annually and updated according to the changing risk environment”.

1.3. In the longer term, the council is considering web-based processing, where card holder information is held only by the payment service providers who have enhanced security in place.

1.4. In the meantime, it is important that the council does not store this sort of data on electronic systems, which may be vulnerable to hacking and other unauthorised access. For this reason, while transaction processing may be carried out electronically, e.g. on credit card terminals, all procedures detailed below which relate to information storage will be paper based.

1.5. These procedures cover the security of credit and debit card related information and must be distributed to all council employees who deal with credit and debit card transactions.

1.6. Management will review and update the procedures at least once a year in line with Requirement 12 to incorporate relevant security needs that may develop.

1.7. Each employee involved must read these procedures and verify that they have read and understood them.

2. Credit and Debit Card Transactions

2.1. Credit Card Terminals

2.1.1. Employees with access to credit card terminals must use them for the intended purposes only and in accordance with the security measures specified with those terminals, including compliance with any anti-tampering rules, ie periodic inspection to look for tampering.

2.1.2. If the customer is not present and the card details are taken over the telephone the transaction must be completed immediately however, if this is not possible, the telephone payment form must be used.

2.1.3. Debit/credit card slips should be placed in the till and then added to the till banking pouches at the end of the day when the tills are ‘cashed up’.

2.2. Mobile Card Payment Terminal

2.2.1. There is a mobile card terminal available to take payments at external events, to be used for the purposes of minimising cash transactions where appropriate.
2.2.2. When not in use the mobile card terminal is stored securely by the Finance Team.
2.2.3. Employees needing to use the mobile card terminal must obtain approval from their Operational Manager before requesting it from the Finance Team and it must be returned following the event.
2.2.4. Employees using the mobile card terminal off the premises must ensure that it is kept securely at all times, use it for the intended purposes only, and in accordance with the security measures specified with those terminals, including compliance with any anti-tampering rules.
2.2.5. Debit and credit card slips should be placed in the cash bag and handed back to the Finance Team following the event, along with the end of period “z” reading report.
2.2.6. A report or statement of sales should also be provided to the Finance Team which details the ledger codes to which the income should be credited, and where applicable, the name of the payer and the invoice number to which the payment relates.

2.3. Telephone Payment Form (DOC 46172) – Finance Office

2.3.1. If the Finance team takes cardholder details directly from a customer they should use this form.
2.3.2. The Telephone Payment form will typically be used where customers are paying invoices for services received.
2.3.3. The Finance Officer will complete the payment and generate the transaction receipt; a hard copy is retained for reconciliation purposes and an electronic copy sent to the customer via email.

3. Protection of Stored Data

3.1. All sensitive information must be stored securely and disposed of in a secure manner when no longer required for business reasons.
3.2. Only paper media should be used to store sensitive information, and it must be protected from unauthorised access.
3.3. Media no longer needed must be destroyed in a manner to render sensitive data irrecoverable (e.g. shredding).

4. Point of sale

4.1. All sensitive information must be stored securely in the till or safe, with access limited to those properly authorised (see below).
4.2. Credit and debit card information should never be retained in the safe for longer than 24 hours (unless over a weekend or Bank Holiday).
4.3. If there is a delay between taking the card holder details and completing the transaction in the till the telephone payment form must be used.

4.4. Card security code information must be destroyed as soon as it has been used for a particular transaction.

5. Credit and Debit Card Information Handling Specifics

5.1. It is prohibited to store the card security or CVC code on any media whatsoever except the tear-off strip from the Telephone Payment Form.
5.2. It is prohibited to store cardholder information on PCs or any other electronic media; such information must be destroyed when no longer needed by shredding or other means of physical destruction.
5.3. Cardholder information is defined as:-
- Card account number
- Expiry date
- Cardholder name (in conjunction with the above)

5.4. The card security or CVC code must never be stored with the cardholder information.
5.5. Once the card security or CVC code information has been matched with appropriate cardholder information and the transaction has been processed, the card security or CVC code must be destroyed.

6. Protection of Data in Transit

6.1. Sensitive information must never be transported electronically.
6.2. Physical transport must always be via a trusted and secure method e.g. by agreed Finance Team procedure.

7. Restriction of Access to Data

7.1. Access to sensitive information is restricted to those who have a need to know.
7.2. No employees should have access to card account numbers unless they have a specific job function that requires such access which will be agreed with their Line Manager.
7.3. Before authorising an employee to handle credit and debit card transactions, the Operational Manager must be satisfied that the employee has read and understood the procedures, and understands how it affects their job.

8. Physical Security

8.1. Physical access to sensitive information must be restricted to protect it from those who do not have a need to access that information.
8.2. Media containing sensitive information must be securely handled and distributed.
8.3. Media containing stored sensitive information must be properly inventoried and disposed of when no longer needed for business reasons.

9. Security Management Plan

9.1. These procedures are subject to the Financial Regulations and Internal Financial Controls.
9.2. In the event of a compromise of sensitive information, the RFO will oversee the execution of the incident response plan.

10. Incident Response Plan

10.1. If a compromise to the security of credit or debit card information is suspected, alert the RFO.
10.2. The RFO will conduct an initial investigation of the suspected compromise.
10.3. If a compromise of information is confirmed, the RFO will alert management and begin informing parties that may be affected by the compromise. If the compromise involves card account numbers, the RFO will perform the following:
- Contain and limit the extent of the exposure by shutting down any systems or processes involved in the compromise
- Alert necessary parties (Merchant Bank, Visa Fraud Control, the police, etc)
- Provide compromised or potentially compromised card numbers to Visa Fraud Control within 24 hours.