Caerphilly County Borough Council

PCI DSS Policy

Version Number:	1.0
Author:	PCI DSS Forum
Last Updated:	24th February 2016

A greener place to work
Man gwyrddach i gweithio

Document Control Information

Document Details	
Department	Human Resources
Title	PCI DSS Policy
Version	1.0
Owner	PCI DSS Forum
Approved By	
Last Updated	24th Feb 2016
Review Frequency	1 year or as required

Revision History				
Version	**Status**	**Date**	**Description**	**Revised By**
0.1	Draft	22 Feb 2012	Initial draft for review	W Colyer
0.2	Draft	30 Mar 2012	Following review by distribution list	W Colyer
0.3	Draft	10 Sep 2012	Added appendices	W Colyer
0.4	Draft	08 Oct 2012	Following review by distribution list	W Colyer
0.5	Draft	25 Jan 2013	Following review by distribution list	W Colyer
0.6	Draft	17 Jul 2014	Following review by distribution list	W Colyer
0.7	Draft	7 Oct 2014	Appendices included within policy	S Jordan
1.0	Final	24 Feb 2016	Annual review	S Jordan

Distribution List	
Version	**Name(s)**
0.1-0.3	PCI DSS Forum
0.4	PCI DSS Forum, IT Security Forum, David Titley, Lesley Edwards, Martin Cook
0.5	PCI DSS Forum, Sian Jones, Jeff Reynolds, Stephen Harris, David Regan
0.6	PCI DSS Forum, Corporate Management Team
0.7	PCI DSS Forum Chair D Regan
1.0	PCI DSS Forum Chair S Jordan

Non-disclosure: The information contained in this document is for internal use only.

Table of Contents

1 Introduction

1.1 Background

The Payment Card Industry Data Security Standard (PCI DSS) is a global standard, founded to assist businesses that process card payments prevent fraud, through increased controls around the data and its exposure to compromise. PCI DSS applies to everyone that stores, processes, or transmits cardholder data.

The Council is liable to fines passed on from its acquiring bank should it fail to comply with PCI DSS, or suffer a breach of the standard. Subsequently card payments may be refused leading to loss of revenue for all service areas.

1.2 Purpose

This document is necessary to comply with the requirements of PCI DSS. It sets out what is permitted, prohibited, and procedure when processing card payments or generally handling cardholder data and associated security of data and equipment.

1.3 Scope

This document is mandatory for all persons in a position of processing card payments or handling cardholder data on behalf of the Council, regardless of if they use that privilege. Included in scope are line managers who may not have a direct input but are responsible for such persons, and must have an equal understanding of what their staff must abide by. Other staff who do not handle card payments but have responsibility for security of premises, equipment and infrastructure should also be aware of this policy.

1.4 Roles and Responsibilities

It is the responsibility of the **PCI DSS Forum** to ensure this document remains accurate, relevant, and available to those persons in scope. The document shall be reviewed according to the frequency set; persons in scope will be required to agree to updated versions and governed to be in adherence.

The **persons in scope** are responsible for complying with all aspects of the document, referring to related documents, and any other associated operational guidance documents as relevant to their duties, and referring back to these documents at any time in doubt.

Line managers must be aware of this document, related documents and any other associated operational guidance documents on which their staff rely. All staff changes must be brought to the attention of the PCI DSS Forum, and no new members of staff are to process cardholder data until they satisfy the training and policy requirements. Any local procedures or processes must be verified to comply with this document.

1.5 Related Documents

- PCI DSS Awareness Guide
- Information Security Policy
- Record Retention and Disposal Policy
- Operating Instructions and Terms of Service of the Council’s bank / card merchant

1.6 Breach of Policy

Failure to comply with this policy, or any guidelines and procedures that implement it, may result in disciplinary and legal action.

2 Policy

2.1 General

2.1.1 All card processing activities of the Council must comply with PCI DSS, no activity or technology may obstruct compliance with the standard.

2.1.2 No new methods of accepting card payments are to be procured without first bringing it to the attention of the PCI DSS Forum, who will align the requirement with the Council’s compliance processes.

2.1.3 All persons must adhere to this policy, any associated operational guidance documents and any specific instructions which may be issued by the PCI DSS Forum to minimise the risk to both customers and the Council.

2.1.4 All persons directly within scope and any other relevant staff must complete the awareness training and sign this policy in writing or electronically, prior to being authorised to process cardholder data.

2.1.5 For all transactions processed, it is strictly prohibited for the Council to store Sensitive Authentication Data (SAD) under any circumstance.

2.1.6 Transactions must be processed according to the operating instructions and terms of service of the Council’s bank / card merchant.

2.1.7 It is prohibited to use cardholder data for any purpose other than completing the transaction requested by the customer.

2.1.8 All persons will protect and never share their username and password for logging in to any IT system specifically those used for processing card payments.

2.1.9 All persons shall have due regard to the security of premises and equipment used to process card payments and should ensure that appropriate and relevant security procedures are in place. Refer to any site and/or equipment specific instructions provided.

2.1.10 For the avoidance of doubt any queries or issues not addressed in this policy, training or associated guidance should be referred to the PCI DSS Forum without delay.

2.2 Accepted Payment Cards

2.2.1 The Council accepts only MasterCard and Visa provided under the corporate merchant service; it does not under any circumstances accept American Express, JCB, or Discover Financial Services cards or any other cards that are not in this list.

2.2.2 Line managers must not under any circumstance, negotiate or otherwise enter into any local agreement with another acquirer for card income processing.

2.3 Cardholder Present Transactions

2.3.1 If a transaction is processed successfully, store the merchant receipt securely (see 2.5) and give the customer receipt to the customer.

2.3.2 If a transaction is declined, advise the customer immediately and offer the option of paying with a different card or alternative means. Store the merchant receipt securely (see 2.5) and give the customer receipt to the customer.

2.3.3 Unless alternative means of payment can be made the customer should be asked to return at another time, never record cardholder data elsewhere (see 2.5.10).

2.3.4 If the PDQ machine is unavailable, offer the customer the option to pay by alternative means, otherwise request they return when it is expected the service will be functioning.

2.3.5 If you receive any notification from the merchant service stating a transaction may be questionable, follow the advice provided in the operating instructions and terms of service of the Council's bank / card merchant.

2.4 Cardholder not Present Transactions

2.4.1 When cardholder data is provided during a telephone call, it must be processed directly into the PDQ machine or IT system and never recorded elsewhere (see 2.5.10). If the appropriate system is unavailable, a call back must be requested or offered.

2.4.2 When cardholder data is provided during a telephone call, it must not be repeated back to the customer in such a way as to be audible to others. If necessary ask the customer to repeat the information.

2.4.3 It is prohibited to request or agree to a customer providing their cardholder data in writing, this includes but may not be limited to fax, letter, email or booking form.

2.4.4 If in receipt of unsolicited cardholder data provided by a customer, the requested transaction must be processed directly into the PDQ machine or IT system and the originating document immediately disposed of securely (see 2.6). If the appropriate system is unavailable, you must dispose of the data securely (see 2.6) as soon as possible, and advise the customer. If the cardholder data was provided in an email, ensure it is not contained within a reply.

2.4.5 If a transaction is processed successfully, provide the customer with the authorisation code.

2.4.6 If a transaction is declined, advise the customer and offer the option of paying with a different card or alternative means. You must store the merchant receipt securely (see 2.5) and offer to send the customer receipt to the customer in the post.

2.4.7 If the customer does not wish to receive their receipt dispose of it securely (see 2.6) as soon as possible.

2.4.8 If a transaction is declined, and the customer has attempted to make payment online and is subsequently querying the transaction; the customer should be instructed to contact their card provider in the first instance. The most common reasons for a declined transaction are the card provider suspecting the transaction may be fraudulent or insufficient funds.

2.4.9 If notification is received from the merchant service stating a transaction may be questionable, follow the advice provided in the operating instructions and terms of service of the Council’s bank / card merchant.

2.5 Storage of Cardholder Data

2.5.1 Secure storage of merchant receipts is defined as:

- Within a locked till, cash box or drawer (temporary store during the working day) at a manned / secure cashiering point. Users of a mobile PDQ machine must store receipts in a zipped waist bag on their person at all times.
- Within a locked safe (permanent store at the end of each working day).

2.5.2 A safe suitable for this purpose is defined as:

- Enough capacity to store the anticipated volume of merchant receipts for the specified retention period (see 2.5.5) with room for expansion.
- Floor-standing secured to the floor and/or wall (preferably into concrete) or, one that would require specialist lifting equipment to be moved.

2.5.3 Safes should be located in a locked room, access to the safe restricted to authorised persons only (a dedicated safe may be required).

2.5.4 You must maintain a Receipt Access Log (see Appendix A), to be stored alongside the merchant receipts in the safe.

2.5.5 Customer contact details must never be stored along with merchant receipts, e.g. receipt attached to a completed booking form including the name and address of the customer. It is also prohibited to write this information on the back of receipts.

2.5.6 Merchant receipts must be retained onsite for a rolling 7 month period for audit purposes and in case of a request for refund or charge back. The receipts must be filed in chronological order, and those older than 7 months must be disposed of securely (see 2.6). Retention relates to merchant receipts only and not other financial records which may need to be retained for much longer.

2.5.7 You must archive each day's receipts in a separate envelope and mark the envelope accordingly (see Appendix C).

2.5.8 Merchant receipts must never be transported off site for storage or disposal, or for any other purpose other than if they are required by Income Officers for chargeback. In these circumstances the receipt(s) must be transported in person by a member of staff in scope of this policy, to Income Officers as approved by the Senior Income Officer, Principal ICT Security Officer, Head of Corporate Finance, Section 151 Officer or Internal Audit Manager at an agreed date and time. These receipts will be retained indefinitely in Income Administration.

2.5.9 Merchant receipts must only otherwise ever be requested and permitted to be seen for any other purpose, by Internal Audit (see 2.8) or Income Officers.

2.5.10 Storage of cardholder data in any format (writing, electronic or voice) is prohibited (e.g. for future processing if systems are unavailable) other than through a PDQ machine or IT system as per operating instructions. This includes but is not limited to fax, email, scanned documents, spreadsheets, written documents and voicemail. Any unsolicited records found must be disposed of securely (see 2.6) as soon as possible.

2.6 Disposal of Cardholder Data

2.6.1 You must securely dispose of merchant receipts, unwanted customer receipts and any other relevant paper based record using a cross cut shredder and in accordance with the Record Retention and Disposal Policy.

2.6.2 You must maintain a Receipt Disposal Log (see Appendix B), to be stored alongside the merchant receipts in the safe.

2.6.3 You must dispose of unsolicited emails containing cardholder data by deleting them from the Inbox and subsequently emptying the Deleted Items folder.

2.6.4 You must dispose of any other electronic records by selecting the file(s), hold down the shift key and press the delete key at the same time to delete files without going to the Recycle Bin. Alternatively empty the Recycle Bin immediately.

2.6.5 Any cross cut shredders found to be defective must be replaced as soon as possible.

2.7 Refunds

As a general rule any refunds of income paid by debit or credit card MUST be refunded back to the paying card. If for any reason this cannot take place this should be recorded and documented.

2.7.1 Online Refunds

2.7.1.1 The refund must be approved by an authorised signatory for the cost centre, who needs to complete the relevant refund form. The form is then passed to an officer in the Cashier's Administration Section, where the refund will be carried out. The appropriate system will be accessed and the refund will be processed back to the source card from which the original transaction was authorised. Confirmation of the refund will be e-mailed to the authorised signatory.

2.7.1.2 If a transaction is older than 90 days, a refund can not be processed to the source card for the original transaction. This is due to security measures implemented by the Payment Service Provider (PSP). In this instance the customer should be contacted for alternative details for the refund to be processed by BACS or cheque.

2.7.1.3 Any section or department guidance in respect of refunds must comply with this policy, however additional processes or records required for departmental administration are permissible provided that Card Data is not recorded.

2.7.2 PDQ Refunds

2.7.2.1 For detailed guidance refer to the operating instructions and terms of service of the Council's bank / card merchant.

2.7.2.2 PDQ refunds require to be authorised on the PDQ machine using a "Supervisor Card". This card must be kept securely by an authorised signatory.

2.7.2.3 The refund must be approved by an authorised signatory for the cost centre. The refund should then be processed through the PDQ machine back onto the source card from which the original transaction was authorised.

2.7.2.4 If the source card is unavailable the reasons should be recorded and if necessary passed to the PCI DSS forum for review then the customer should be asked for alternative details for the refund to be processed by BACS or cheque.

2.7.2.5 A refund must never be processed onto a card that is not the source transaction card, confirm the source card by accessing the relevant merchant receipt.

2.8 Validation and Monitoring

2.8.1 The Council will validate its compliance against the latest version of PCI DSS through annual Self-Assessment Questionnaire (SAQ) reviews.

2.8.2 The Council will also validate its compliance by contracting an Approved Scanning Vendor (ASV) to perform a vulnerability scan at least quarterly, of its systems which process cardholder data.

2.8.2 Sites will be visited at least once annually by Internal Audit, actions will be formally recorded and follow up visits arranged if necessary. Visits may not always be made with prior notice.

2.8.3 Line managers and staff will immediately be made aware of any identified breaches of this policy together with instructions to remedy such breaches. All breaches will also be reported in accordance with section 3.

2.8.4 It is expected such instructions will be adopted immediately, further action to improve procedures, processes or equipment may be considered if necessary.

2.8.5 The PCI DSS Forum will meet regularly to discuss Internal Audit reviews, changes to PCI DSS or changes in our systems and personnel. Meeting minutes will be made available to the IT Security Forum and relevant senior management.

2.8.6 The IT Security team may run software to scan computers and network drive locations for cardholder data and sensitive authentication data stored electronically.

2.8.7 The Council 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.

3 Incident Reporting

In the event of there being a breach of security of cardholder data in any way, you must contact the IT Security team as soon as possible. Any weaknesses found in systems or processes which may have a later impact must also be reported. Security incidents will be handled in accordance with ISO/IEC 27001 international standards.

E-mail:	itsecurity@caerphilly.gov.uk
Telephone:	01443 863224 / 3227

4 Declaration

NB: To be completed only whereby a hardcopy has been issued.

I acknowledge I have read, understood and will comply with this document. I understand that failure to do so may result in disciplinary and legal action.

Name in full (print)	
Job title	
Signature	
Date	

5 Further Information

The PCI DSS Forum welcomes feedback and encourages readers to inform us of their experiences, good or bad in this document. We would especially like to be informed of any inconsistencies and ambiguities, or if you have difficulties implementing or complying with any aspect of the document. Please refer to the Intranet for up-to-date documentation.

The Income Administration team are the primary contact for the PCI DSS Forum.

E-mail:	cashadmin@caerphilly.gov.uk
Telephone:	01443 863351

For all other queries, contact the IT Helpdesk:

Email:	ithelpdesk@caerphilly.gov.uk
Telephone:	01443 86(4111)

The PCI Security Standards Council (PCI SSC) provide a wealth of material on their website including the latest news and FAQs, you can access the website using the following URL:

https://www.pcisecuritystandards.org/

Appendix A - Receipt Access Log

PCI DSS Policy

Merchant receipts which have been archived must be accessed in accordance with the PCI DSS Policy, additionally:

- Before accessing receipts, you must satisfy the following requirements:

    - You are an employee of Caerphilly CBC in scope of the PCI DSS Policy.

    - A colleague is available to act as witness. If you are working alone or do not have a colleague who may act as witness, annotate the envelope accordingly as ‘unwitnessed’.

    - You have obtained the envelope for the correct day.

    - Your reasons for accessing the receipts should be limited to:
        - Processing a refund or chargeback;
        - Internal audit checks or to satisfy requests from Income Officers;
        - Disposal (see section 2.6 of the PCI DSS Policy).

    - A log entry must be created for every receipt removed / added i.e.:
        - A receipt is considered removed if taken from an envelope for any reason, other than disposal purposes (there is no need for a log entry if you are disposing of receipts according to the PCI DSS Policy;
        - A receipt may be added if for any reason it was not available at the time that day was archived;
        - A receipt removed constitutes only one entry even if it is returned, the description must provide an appropriate account of your reason.

- Following access reseal the envelope and mark it with your signature and the signature of your colleague acting as witness (if available) across the seal (see the Archived Receipts Envelope Template, appendix C of the PCI DSS Policy).

- If an envelope is damaged or cannot be resealed for any reason, follow the Archived Receipts Envelope Template procedure using a new envelope, retain the previous envelope for auditing purposes (combine envelopes with an elastic band).

- You must retain log entries for 24 months on a rolling basis.

- You may destroy log sheets only when the most recent entry on the sheet is more than 24 months ago.

- This log must be printed and completed in ink, it should also be:

    - stored securely along with the receipts;

    - made available for inspection by Internal Audit or Income Officers upon request.

Here is an example of a completed log entry, a receipt was removed on 1st June for the purpose of processing a refund:

Date of access:	01/06/12	**Date of receipt:**	15/05/12	**Receipt auth code:**	000001
Your name (print):	A. Name		**Your name (signature):**	A. Name	
Your designation:	Leisure centre assistant				
Reason for access:	Customer refund				

Receipt Access Log

Date of access:	/ /	**Date of receipt:**	/ /	**Receipt auth code:**	
Your name (print):			**Your name (signature):**		
Your designation:					
Reason for access:					

Date of access:	/ /	**Date of receipt:**	/ /	**Receipt auth code:**	
Your name (print):			**Your name (signature):**		
Your designation:					
Reason for access:					

Date of access:	/ /	**Date of receipt:**	/ /	**Receipt auth code:**	
Your name (print):			**Your name (signature):**		
Your designation:					
Reason for access:					

Date of access:	/ /	**Date of receipt:**	/ /	**Receipt auth code:**	
Your name (print):			**Your name (signature):**		
Your designation:					
Reason for access:					

Date of access:	/ /	**Date of receipt:**	/ /	**Receipt auth code:**	
Your name (print):			**Your name (signature):**		
Your designation:					
Reason for access:					

Receipt Access Log

Date of access:	/ /	**Date of receipt:**	/ /	**Receipt auth code:**	
Your name (print):			**Your name (signature):**		
Your designation:					
Reason for access:					

Date of access:	/ /	**Date of receipt:**	/ /	**Receipt auth code:**	
Your name (print):			**Your name (signature):**		
Your designation:					
Reason for access:					

Date of access:	/ /	**Date of receipt:**	/ /	**Receipt auth code:**	
Your name (print):			**Your name (signature):**		
Your designation:					
Reason for access:					

Date of access:	/ /	**Date of receipt:**	/ /	**Receipt auth code:**	
Your name (print):			**Your name (signature):**		
Your designation:					
Reason for access:					

Date of access:	/ /	**Date of receipt:**	/ /	**Receipt auth code:**	
Your name (print):			**Your name (signature):**		
Your designation:					
Reason for access:					

Appendix B - Receipt Disposal Log

Receipt Disposal Log

Merchant receipts must be disposed of in accordance with the PCI DSS Policy, additionally:

- Before disposing of receipts, you must satisfy the following requirements:
    - You are an employee of Caerphilly CBC in scope of the PCI DSS Policy.
    - A colleague is available to act as witness. If you are working alone or do not have a colleague who may act as witness, annotate the log accordingly as ‘unwitnessed’.
    - You have obtained all envelopes for the necessary month.
    - You have examined the envelopes and their seals and they do not bear any signs of having been opened or otherwise tampered with.
    - If an envelope has been opened then there is a record in the Receipt Access Log to support this, and the envelope has been resealed as per the Archived Receipts Envelope Template.
    - If an envelope has been opened and there is a discrepancy, or signs of tampering, report it as per the PCI DSS Policy under Incident Reporting.
    - A count of receipts inside each envelope matches the number recorded on the front of the envelope.
        - If there is a discrepancy can it be accounted for in the current Receipt Access Log?
        - If there is a discrepancy and it cannot be accounted for, report it as per the PCI DSS Policy under Incident Reporting.
    - If subsequently you find any envelopes which should already be disposed of, make an additional log entry and include an explanation in the notes section.
- You must retain log entries for 24 months on a rolling basis.
- You may destroy log sheets only when the most recent entry on the sheet is more than 24 months ago.
- This log must be printed and completed in ink, it should also be:
    - stored securely along with the receipts;
    - made available for inspection by Internal Audit or Income Officers upon request.

Here is an example of a completed log entry, disposal was carried out on 1st June 2012 of the receipts for October 2010:

Date of disposal:	01/06/12	**Disposal month (e.g. 10/2011):**	10 / 2011	**No. of envelopes:**	20
Your name (print):	A. Name		**Witness name (print):**	A. Witness	
Your signature:	A. Name		**Witness signature:**	A. Witness	
Your designation:	Cashier		**Witness designation:**	Cashier	
Notes:					

Receipt Disposal Log

Date of disposal:	/ /	**Disposal month (e.g. 10/2011):**	/	**No. of envelopes:**	
Your name (print):			**Witness name (print):**		
Your signature:			**Witness signature:**		
Your designation:			**Witness designation:**		
Notes:					

Date of disposal:	/ /	**Disposal month (e.g. 10/2011):**	/	**No. of envelopes:**	
Your name (print):			**Witness name (print):**		
Your signature:			**Witness signature:**		
Your designation:			**Witness designation:**		
Notes:					

Date of disposal:	/ /	**Disposal month (e.g. 10/2011):**	/	**No. of envelopes:**	
Your name (print):			**Witness name (print):**		
Your signature:			**Witness signature:**		
Your designation:			**Witness designation:**		
Notes:					

Date of disposal:	/ /	**Disposal month (e.g. 10/2011):**	/	**No. of envelopes:**	
Your name (print):			**Witness name (print):**		
Your signature:			**Witness signature:**		
Your designation:			**Witness designation:**		
Notes:					

Receipt Disposal Log

Date of disposal:	/ /	Disposal month (e.g. 10/2011):	/	No. of envelopes:	
Your name (print):			Witness name (print):		
Your signature:			Witness signature:		
Your designation:			Witness designation:		
Notes:					

Date of disposal:	/ /	Disposal month (e.g. 10/2011):	/	No. of envelopes:	
Your name (print):			Witness name (print):		
Your signature:			Witness signature:		
Your designation:			Witness designation:		
Notes:					

Date of disposal:	/ /	Disposal month (e.g. 10/2011):	/	No. of envelopes:	
Your name (print):			Witness name (print):		
Your signature:			Witness signature:		
Your designation:			Witness designation:		
Notes:					

Date of disposal:	/ /	Disposal month (e.g. 10/2011):	/	No. of envelopes:	
Your name (print):			Witness name (print):		
Your signature:			Witness signature:		
Your designation:			Witness designation:		
Notes:					

Appendix C - Archived Receipts Envelope Template

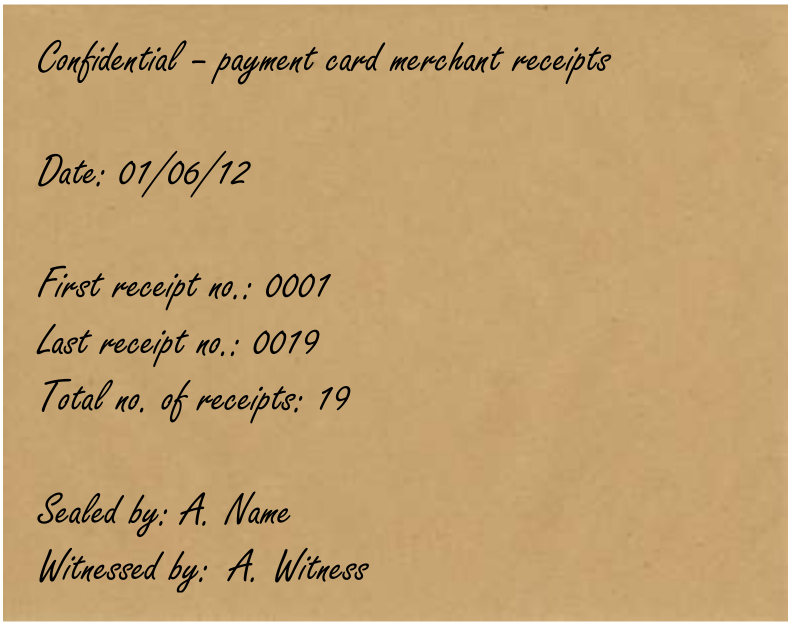
PCI DSS Policy

This document outlines the procedure which must be followed to mark envelopes used to archive merchant receipts as part of daily end of business routines.

- Before archiving merchant receipts, you must satisfy the following requirements:
  - You are an employee of Caerphilly CBC in scope of the PCI DSS Policy.
  - A colleague is available to act as witness. If you are working alone or do not have a colleague who may act as witness, annotate the envelope accordingly as ‘unwitnessed’.
  - Mark the front of the envelope with the following details:
    - ‘Confidential – payment card merchant receipts’;
    - Today’s date;
    - The first and last receipt numbers (if available);
    - Total number of receipts;
    - Your name
    - The name of a colleague acting as witness (if available and in scope of the PCI DSS Policy.
  - Mark the back of the envelope with your signature and the signature of your colleague acting as witness (if available) across the seal.
- As soon as possible each calendar month, combine all envelopes for the previous calendar month with an elastic band (in date order).

This procedure is illustrated in the following example.

Front of envelope:



Confidential – payment card merchant receipts

Date: 01/06/12

First receipt no.: 0001

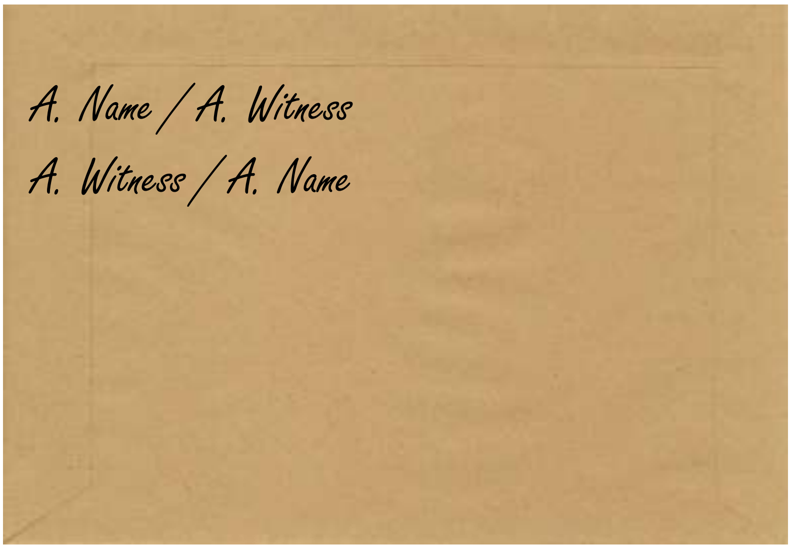
Last receipt no.: 0019

Total no. of receipts: 19

Sealed by: A. Name

Witnessed by: A. Witness

Back of envelope:



A. Name / A. Witness

A. Witness / A. Name

In this example A. Name originally sealed the envelope witnessed by A. Witness.

A. Witness needed to access a receipt within the archive and in doing so must have updated the Receipt Access Log. The envelope is resealed and signed by A Witness, witnessed by A. Name.