Caerphilly County Borough Council

PCI DSS Awareness Guide

Version Number: 1.0

Author: PCI DSS Forum

Last Updated: 11th November 2014

Document Control Information

Document Details	
Department	Human Resources
Title	PCI DSS Awareness Guide
Version	1.0
Owner	PCI DSS Forum
Approved By	
Last Updated	11th November 2014
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

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

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

Introduction

The Payment Card Industry Data Security Standard (PCI DSS) is a set of mandatory requirements to help ensure safe handling of cardholder data.

This guide aims to raise your understanding of PCI DSS and the commitment required from you to ensure the Council is compliant. Through this guide you will learn:

- General awareness of PCI DSS
- Requirements of PCI DSS and how it affects the Council
- PCI DSS requirements which directly affect you
- Identifying 'account data' and how to handle it
- Knowing the equipment and systems you use
- The Council's PCI DSS Policy
- Incident reporting and your responsibilities
- Next steps and who to contact if you have any queries

PCI DSS Glossary

Throughout this guide, PCI DSS Policy, and when discussing or reading about PCI DSS, you are likely to come across the following acronyms and terminology which you may need to understand.

PCI DSS	Payment Card Industry Data Security Standard.
PCI SSC	Payment Card Industry Security Standards Council.
Acquirer	Also referred to as "acquiring bank" or "acquiring financial institution". An entity that initiates and maintains relationships with merchants for the acceptance of payment cards.
Merchant	For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five member card brands as payment for goods or services.
ASV	Approved Scanning Vendor, company approved by the PCI Security Standards Council to conduct external system vulnerability scanning services.

PSP	Payment Service Provider offer services for accepting online payments.
PDQ	Process Data Quickly, the name given to payment terminals used to process card payments, also referred to as “chip and pin” machines.
BACS	Bankers Automated Clearing Service, an automated payment method using dedicated software linked in with the bank’s system.
PAN	Primary Account Number, also referred to as “account number”. Unique payment card number that identifies the issuer and the particular cardholder account.
PIN	Personal Identification Number, numeric password known only to the cardholder which replaces a physical signature to authenticate cardholders present and authorise card payments.
PIN block	When a cardholder enters their PIN, the information is first encoded into a plain text ‘PIN block’, derived from the PIN length, the PIN digits, and a portion of the PAN. The plain text ‘PIN block’ is then encrypted and it is this that is used to verify the payment card.
Card Verification Code or Value (CVC2/CVV2)	Also known as “Card Validation Code” or “Value”, or “Card Security Code”. Refers to either magnetic stripe data, or printed security code features dependent on the payment card brand.
SAD	Sensitive Authentication Data, security related information (including but not limited to card verification code/value, full magnetic-stripe data, PINs, and PIN blocks) which must never be stored.
Cardholder	Non-consumer or consumer customer to whom a payment card is issued to or any individual authorised to use the payment card.
Cardholder data	At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and service code. See SAD for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction.

About the Payment Card Industry Data Security Standard (PCI DSS)

Cardholder data is a tempting target which requires the need for adequate security and increased vigilance to prevent and deter the threat of a data breach. It is a target for fraudsters and a series of high profile security breaches worldwide highlighted a major problem. The problem is a very real threat to businesses engaged in accepting card payments by credit or debit card, potentially unfortunate targets of intelligently orchestrated attacks.

MasterCard and Visa became increasingly concerned with the level of security protecting account and transaction information. They needed to ensure that the level of protection a merchant employs is sufficient to deter hackers and criminals, and so they each produced a set of security standards of their own.

In January 2005, MasterCard and Visa combined their individual security standards for cardholder data to create a joint program, which was then also endorsed by American Express, JCB and Diners (collectively known as the Card Schemes). They formed the PCI Security Standards Council (PCI SSC), an open global forum responsible for the ongoing development, management, education, and awareness of the PCI Security Standards, which PCI DSS is a part of.

PCI DSS requires all business that store, process or transmit cardholder data to comply with 12 requirements, covering both IT security and operational practises. It not only ensures the business has sufficient protection in place to alert and prevent breaches but also continually defend against hackers and criminals. PCI DSS is based on existing International Organisation for Standardisation (ISO) standards, industry best practises and a common sense approach to security.

What Happened Prior to PCI DSS?

This short animated video provides a “tongue in cheek” look at the history of the evolution of payment card security and the PCI Security Standards Council (PCI SSC), the organisation responsible for PCI DSS and other standards for keeping cardholder data secure.

Although this is an optional part of this guide, it may supplement your understanding of why the PCI SSC was formed. The video runs for 2 minutes and 48 seconds.

NB: The video features audio, please consider using headphones or adjusting the speaker volume to a suitable level before playing.

What Are the 12 PCI DSS Requirements?

The requirements are grouped into six related areas, known as the ‘control objectives’.

Build and Maintain a Secure Network

1 Install and maintain a firewall configuration to protect cardholder data

2 Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3 Protect stored cardholder data

4 Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5 Use and regularly update anti-virus software or programs

6 Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7 Restrict access to cardholder data by business need-to-know

8 Assign a unique ID to each person with computer access

9 Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10 Track and monitor all access to network resources and cardholder data

11 Regularly test security systems and processes

Maintain an Information Security Policy

12 Maintain a policy that addresses information security for employees and contractors

Why Should the Council be Compliant?

Compliance with PCI DSS minimises the risk of the Council suffering a security breach of cardholder data, this is important to the Council considering how a breach may result in:

- Loss of customer confidence / reputation possibly leading to loss of revenue
- Lengthy / costly security investigations and corrective actions
- Lack of use of invested technology and the way we take payment for goods and services
- Increased level of fraud in the card market / increased costs for all involved in accepting payment cards
- Disciplinary or legal action against staff
- Substantial fines and costs applied by the Card Schemes
- Loss of PCI DSS compliance

Non compliance with PCI DSS may result in:

- Monthly non compliance fines
- Termination of payment card processing facilities by the acquirer

How Does the Council Become Compliant?

The Council is a merchant as it accepts payment cards for goods and services, operating under multiple merchant numbers which distinguish the different goods and services the Council provide. The Card Schemes divided businesses into 4 levels depending on the volume and type of transactions processed:

- How many card transactions accepted per annum, per card scheme
- Which channels are used to accept those transactions

Based upon current transaction levels, the Council is categorised as a level 4 merchant for which there is a minimum set of compliance requirements from the standard in full. The main requirements are:

- Annual renewal of a Self Assessment Questionnaire (SAQ) evidencing PCI DSS compliance.
- Contract an Approved Scanning Vendor (ASV) to perform a vulnerability scan at least quarterly, of systems which process cardholder data.
- Maintain a policy and conduct training and awareness for staff (at least annually).

- The Council is responsible that all IT systems, Payment Service Providers (PSP), and any other third parties with access to cardholder data comply with the requirements of PCI DSS. The Council may be liable to fines and other associated costs should a security breach occur as a result of third party negligence, and the Council's compliance status may be considered void by the Card Schemes.

PCI DSS Forum

A PCI DSS Forum was formed to lead the Council through its compliance with the standard, it is made up of staff representing IT Security, IT Development, Internal Audit and Income. The forum members meet on a regular basis and report to senior management, on topics including:

- Current compliance status
- Changes to PCI DSS
- New and existing IT systems
- Other changes to the scope of the Council's cardholder environment such as:
    - New sites / merchant numbers
    - Staff changes
    - Additional equipment
- Internal audit results and corrective actions
- Ongoing training and awareness for staff

Contact details for the PCI DSS Forum are provided at the end of this guide.

PCI DSS Requirements That Affect You

Behind the 12 high level requirements are many, much more detailed sub requirements. While not all of them are relevant to you, it is important you understand what is involved.

Technical requirements are the responsibility of IT Services, the PCI DSS Forum oversee these requirements and those which are operational and apply to you.

Requirement 3: Protect stored cardholder data

- Cardholder data can be stored but must be protected, not stored unnecessarily and for a limited retention period. Under no circumstances can Sensitive Authentication Data (SAD) be stored.

Requirement 7: Restrict access to cardholder data by business need-to-know

- Cardholder data must not be accessible to anyone who does not have a business requirement, or if they have not yet satisfied the training and policy requirements.

- Access rights should be reviewed regularly to ensure that staff who have since left their role no longer have access to cardholder data, including IT systems and manual records.

Requirement 8: Assign a unique ID to each person with computer access

- All members of staff are issued with a unique username and password to logon to the network and IT systems, thus enabling traceability.

- It is your responsibility to keep your password secret, never share it, never write it down, and you will be required to change it on a regular basis.

Requirement 9: Restrict physical access to cardholder data

- IT systems and merchant receipts must be physically secured at all times.

- Never allow unauthorised people access to cardholder data.

- Keep merchant receipts out of view at all times not to encourage the opportunist thief.

- During the working day, store merchant receipts in a locked till, cash box or drawer, a physical barrier should exist between you and customers.

- At the end of the working day, store merchant receipts permanently in a locked safe.

Requirement 12: Maintain a policy that addresses information security for employees and contractors

- The Information Security Policy sets out rules by which members of staff must conduct themselves with information.

- This guide will be adapted according to changes to PCI DSS, industry best practises and any need for improvement deemed necessary as a result of internal audits or security incidents.

- This guide will be published to you on at least an annual basis, any other material which may be of benefit will be made available through email circulation and on the Intranet.

- A PCI DSS Policy created by the PCI DSS Forum addresses the controls necessary to meet the requirements of PCI DSS and additional measures aimed at significantly minimising risk.

- The PCI DSS Policy will be regularly reviewed and updated as and when necessary, at this time it will be re-published to you for your acceptance.

- The IT Services department is committed to preserving the confidentiality, integrity and availability of its information assets.

What is Account Data?

Account data consists of cardholder data plus SAD, this table is an extract from the PCI DSS requirements document and highlights what can and cannot be stored.

	Data Type	Storage Permitted?	Protection Required?
Cardholder Data	Primary Account Number (PAN)	YES	YES
	Cardholder Name	YES	YES
	Expiry Date	YES	YES
	Service Code	YES	YES
Sensitive Authentication Data (SAD)	Full Magnetic Stripe	NO	N/A
	3 or 4 digit Security Code (CVC2/CVV2/CID)	NO	N/A
	PIN / PIN Block	NO	N/A

NB: SAD must never be stored subsequent to authorisation, even if it is encrypted. As a minimum the PAN must be unreadable (including data on backup media and in logs) and can only be stored through the use of encryption. All data should be destroyed once it is no longer required (PCI DSS Policy controls retention).

Identifying Account Data

Equipment and Systems

The Council accepts card payments in a number of ways, for a wide range of goods and services such as gifts, tickets, leisure services, council tax and parking fines. It is clear to see how PCI DSS compliance is critical to the good reputation and financial health of the organisation.

You may be responsible for accepting card payments via a PDQ machine or IT system, cardholders may be present or they may not, you may deal with more than one scenario so it is important you are a competent user of the technology.

Therefore you must ensure through your line manager, that you are provided with adequate training on the technology you will use. Familiarise yourself with any local procedures or processes, and any other associated operational guidance documents you need to be made aware of.

Local procedures or processes must be verified to comply with the PCI DSS Policy and any subsequent changes may need to be brought to the attention of the PCI DSS Forum.

A lack of training in these areas will only increase the risk of a breach of PCI DSS Policy or other related security incident which may compromise compliance for the entire Council.

No new equipment or IT systems are to be procured without first contacting the PCI DSS Forum. The Council accepts only MasterCard and Visa cards through its acquiring bank, no negotiations or local agreements with another acquirer are permitted for card income processing.

The risk to cardholder data isn't all about cyber criminals attempting to hack into our network from afar. There is the risk that cardholder data is compromised at the point of payment, by means of tampering to the physical equipment.

You may have heard about card skimming devices attached to cash point terminals, in a similar fashion a criminal may attempt to tamper with or even replace a PDQ terminal in order to capture cardholder data.

It is therefore important that you consider the following good practices:

- Regularly check equipment for signs of tampering, marks or other visual differences such as a change of cabling or extra hardware must be reported;
- Periodically compare equipment specific information with records kept such as serial number and asset number (if applicable);
- Confront any non authorised persons found handling the equipment, and first confirm with the Income Administration team anyone who claims to be needing to repair or replace it;
- Make use of any security controls provided to protect equipment when not in use, especially in environments openly accessible to the public.

PCI DSS Policy

The PCI DSS Policy with which you must abide sets out the do's and don'ts when processing or generally handling cardholder data. Since the policy is so descriptive this page serves as a brief overview only.

Sections in the policy include:

- Accepted Payment Cards
- Cardholder Present Transactions
- Cardholder not Present Transactions
- Storage of Cardholder Data
- Disposal of Cardholder Data
- Refunds
- Validation and Monitoring
- Incident Reporting

What Happens Next?

PCI DSS is an enabler for the Council to be able to accept card payments, it will evolve and continue to change as fraudsters identify new ways to compromise cardholder data.

You are directly responsible in helping the Council comply with the standard, which will be an ongoing process to minimise the associated risks. Please be vigilant at all times and proactive in reporting any security incidents no matter how trivial. You may suspect there has been a breach of the PCI DSS Policy, or compromise of cardholder data - report it.

Once you have completed this guide, the PCI DSS Policy will be published to you in the same way for your acceptance. It is available on the Intranet if you wish to read it beforehand. Once you have agreed to the PCI DSS Policy you are then authorised to take payments by credit or debit card, but you must also ensure with your line manager that you have had adequate training in using the IT systems and any other equipment / processes that will be part of your responsibilities.

Raising awareness of PCI DSS must be done on a regular basis therefore to maintain your level of understanding you will periodically (at least annually) receive this guide and the PCI DSS Policy again. Should you have any ideas for improvement then please contact the PCI DSS Forum, contact details are provided on the next page.

The final step in this guide involves answering a short quiz, to test your understanding of PCI DSS based on the material in this guide.

Further Information

This guide and other supplementary guidance on PCI DSS is available on the Intranet.

The PCI DSS Forum welcomes feedback and encourages readers to inform us of their experiences, good or bad in this guide. We would especially like to be informed of any inconsistencies and ambiguities.

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 Help Desk:

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

The 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 – PCI DSS Awareness Guide Quiz

<Insert quiz>