



PAYMENT CARD DATA POLICY

Metadata

Author.Contributor	Derrick Bates
Coverage.spatial	UK, Cumbria
Creator	ICT Client Team Organisational Development
Date.issued	01 May 2008
Description	The document sets out the corporate policy on the processing and use of payment card data
Format	Txt
Identifier	
Language	Eng
Publisher	Cumbria County Council
Rights.copyright	Cumbria County Council
Status	Version 1.0 Final
Subject.category	Information & Computer Security
Subject.keywords	Information management; resources; retrieval; policy; security; users; credit card; debit card; pcidss; payment;
Title	Cumbria County Council Payment Card Data Policy

Distribution

Issue Date	Version	Name	Title

Revision History

Document ID.version	Status	Date	Reason for review	Author
v0.1	Draft	2008-01-07	Initial creation	D Bates
V0.2	Draft	2008-01-25	Amended	D Bates
V0.3	Draft	2008-03-14	Further amendments	D Bates
V 1.0	Final	2008-05-01	Final	D Bates

Approval

Name	Position	Date	Signature

This Policy will be reviewed by the corporate Information Technology Security Officer annually from the date of approval.

Table of Contents

1	INTRODUCTION	4
2	OBJECTIVE	4
3	SCOPE	4
4	POLICY	4
4.1	Compliance	4
4.2	Monitoring	5
4.3	Policy Maintenance and Review	5
5	APPENDIX 1 – PRINCIPLES OF PCIDSS.....	6

1 Introduction

The use of credit, debit and other types of payment cards for the payment of transactions both personally and online via the Internet is now a ubiquitous part of our society. It is also one of the principle means whereby security can be compromised and identity theft carried out. To aid in countering this threat the Payment Card Industry Data Security Standards (PCIDSS) were introduced with compliance set for December 2008

All parts of the Council that take payments from customers using payment cards are required to abide by the principles of the PCIDSS. These principles can be seen at Appendix 1.

2 Objective

It is the objective of this policy to ensure customer payment card data is secure and protected.

3 Scope

This document defines Cumbria County Council's policy for the use and handling of customer payment card data. It does not lay down absolute procedures for departments to follow. It does not apply to cash payments used to satisfy transactions. This policy applies to all Members and employees, consultants, temporary or contract workers working for the Council.

4 Policy

4.1 Compliance

It is the Policy of the Council that Directorates processing card payments on behalf of customers will comply with all principles and aspects of the Payment Card Industry Data Security Standards. Where the Standards refer to technical aspects of the infrastructure used to process the card data it is the Policy of the Council that the Strategic ICT Partner will be responsible for such compliance. As at the date of this policy that Partner is Agilisys.

4.2 Monitoring

All users processing card data are required to be signatories to the Corporate Acceptable Use Policy (AUP). Monitoring of systems use carried out under the aegis of the AUP will include checking adherence to the PCIDSS.

4.3 Policy Maintenance and Review

This policy will be reviewed and updated annually from the date of issue. If the PCIDSS are updated during the interim period the policy will be updated to reflect any changes.

5 Appendix 1 – Principles of PCIDSS

Task Area	Item No.	Requirement	Owner
Build and maintain a secure network	1	Install and maintain a firewall configuration to protect cardholder data	Strategic ICT Partner
	2	Do not use vendor-supplied defaults for system passwords and other security parameters	Strategic ICT Partner
Protect cardholder data	3	Protect stored cardholder data	CCC and Strategic ICT Partner
	4	Encrypt transmission of cardholder data across open, public networks	CCC
Maintain a vulnerability management program	5	Use and regularly update anti-virus software	Strategic ICT Partner
	6	Develop and maintain secure systems and applications	Strategic ICT Partner
Implement strong access control measures	7	Restrict access to cardholder data by business need-to-know	CCC
	8	Assign a unique ID to each person with computer access	Strategic ICT Partner
	9	Restrict physical access to cardholder data	CCC and Strategic ICT Partner
Regularly monitor and test networks	10	Track and monitor all access to network resources and cardholder data	CCC and Strategic ICT Partner
	11	Regularly test security systems and processes	CCC and Strategic ICT Partner
Maintain an information security policy	12	Maintain a policy that addresses information security	CCC