



Corporate Policy and Resources Committee
Date: 13 April 2017

Subject: Implementation of PCI-DSS Security Policy

Report by:	Director of Resources
Contact Officer:	Steve Anderson Information Governance Officer 01427 676652 Steve.anderson@west-lindsey.gov.uk
Purpose / Summary:	The purpose of this report is to introduce a new Council policy to comply with the PCI-DSS standard

RECOMMENDATIONS: 1) That members, approve the attached PCI-DSS Security Policy for formal adoption. 2) That delegated authority be granted to the SIRO to make minor house-keeping amendments to the Policy in the future, in consultation with the Chairpersons of the Joint Staff Consultative Committee and the Corporate Policy and Resources Committee.

IMPLICATIONS

Legal: This report has direct positive implications on the Council's compliance with the Payment Card Industry Data Security Standard.

If an organisation loses card data and is not PCI DSS compliant then there is the potential for financial penalties to be imposed such as:

- fines for the loss of this data;
- fraud losses incurred against the cards involved; and
- bank operational costs associated with replacing the accounts.

Financial: None from this report

Fin Ref: [FIN/1/18](#)

Staffing : None from this report

Equality and Diversity including Human Rights:

None from this report

Risk Assessment: None

Climate Related Risks and Opportunities : None from this report.

Title and Location of any Background Papers used in the preparation of this report:

Call in and Urgency:

Is the decision one which Rule 14.7 of the Scrutiny Procedure Rules apply?

i.e. is the report exempt from being called in due to urgency (in consultation with C&I chairman)

Yes

No

X

Key Decision:

A matter which affects two or more wards, or has significant financial implications

Yes

No

X

1. Background

The Payment Card Industry Data Security Standard (PCI DSS)

1.1 PCI DSS is a worldwide standard that was set up to help businesses process card payments securely and reduce card fraud. It does this through tight controls surrounding the storage, transmission and processing of cardholder data that businesses handle. PCI DSS is intended to protect sensitive cardholder data. If an organisation loses card data and is not PCI DSS compliant then there is the potential for financial penalties to be imposed such as:

- fines for the loss of this data;
- fraud losses incurred against the cards involved; and
- bank operational costs associated with replacing the accounts.

1.2 Customers may also opt for alternate, more resource intensive payment methods. As the Council takes a substantial number of payments by card (21,153 between Apr 2016 and Nov 2016) this would have a detrimental effect on the Medium Term Financial Plan.

1.3 Requirement 12 of the Standard requires all organisations who take card payments to:

“Maintain a policy that addresses information security for all personnel. A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.

For the purposes of Requirement 12, “personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are “resident” on the entity’s site or otherwise have access to the cardholder data environment.”

1.4 This report presents a **NEW** Policy to comply with Requirement 12.

1.5 The Policy will be a sub-policy of the Council's IT Security Policy and, while essentially standalone, must be read and applied in conjunction with other policy documents in the set. It has been developed with advice and assistance from Internal Audit and relevant experts in the Council and supports a number of recommendations in the recent PCI DSS Compliance Internal Audit Report dated December 2016.

2. Scope

2.1 The Policy applies to staff, contractors and third parties who access the Council's Cardholder Data Environment (CDE) for the purposes of taking payments or maintaining the payment systems.

3. The Policy

The Policy is relevant to the Council's 3 methods of taking card payments:

1. Web Payments (Cardholder Not Present).
2. Face to Face Card Payments (Cardholder Present).
3. Self-serve Kiosk in Customer Services.

The document has been structured to comply with the PCI DSS Standard with sections for the following:

- General policy statements;
- Handling of credit cards;
- Physical security;
- Acceptable use; and
- Responsibilities.

Appendix 1 of the Policy provides information on the card readers in use in the Council to enable staff to inspect the devices for tampering or damage.

4. Policy Implementation

All staff, contractors and third parties who access the Cardholder Data Environment either to take payments or maintain our payment systems will be required to read and sign this Policy. They will also be required to undertake specialist PCI-DSS training on our Corporate Learning Platform.

5. Decisions Required

- 1) That members, approve the attached Information Governance Policy, Legal Responsibilities Policy and Information Sharing Policy for formal adoption.
- 2) That delegated authority be granted to the SIRO to make minor house-keeping amendments to the Policy in the future, in consultation with the Chairmen of the Joint Staff Consultative Committee and the Corporate Policy and Resources Committee.



PCI-DSS Security Policy

Table of Contents

1	Overview.....	3
2	Purpose	3
3	Scope	3
4	Policy	3
4.1	General	3
4.2	Credit Card Handling.....	4
4.2.1	Scope	4
4.2.2	Policy Statements	4
4.3	Physical Security	7
4.3.1	Device Checking.....	7
4.3.2	Personnel Checking	7
4.4	Acceptable Use	8
4.5	Responsibilities	8
5	Policy Compliance	9
5.1	Compliance Measurement	9
5.2	Exceptions.....	9
5.3	Non-Compliance	9
5.4	Policy Review.....	9
6	Related Standards, Policies, and Processes	9
	Appendix 1 - Detecting Evidence of Device Tampering	10
	Device Details	10
	Reverse Side Unique Identification Labels	11
	Reverse Side Connectors	12
	Screw Positions	13
	Left Side Tether	13
	POI Weights	13
	Inspecting the Device	13
	Example of an Inspection Log of all Card Machines.....	14

1 Overview

This Policy provides essential information for everyone tasked with handling credit and debit cards, credit and debit card data and the systems processing such data within West Lindsey District Council (the Council).

2 Purpose

The Policy is designed to make sure we can meet the standards required by the Payment Card Industry's Data Security Standard (PCI-DSS), which the Council is obliged to meet in order to be able to process credit card payments.

3 Scope

All environments within the Council where credit and debit cards are handled.

4 Policy

4.1 General

- System users shall not send confidential data, such as credit or debit cardholder data, unencrypted, via end-user messaging technologies such as, e-mail, instant messaging or chat without using an approved encryption solution. Where a solution is not available the data shall not be sent via any of these methods.
- All employees, 3rd parties or contractors shall not attach or use within the Council's cardholder data environments network devices including but not limited to modems, remote-access technologies, wireless technologies, removable electronic media, personal laptops, tablets, PDAs, iPods or personal storage media (e.g. memory sticks).
- Users shall not store confidential data, such as credit and debit cardholder data on local hard drives, USB sticks, or other external or mobile media. If anyone must store confidential data on a hard disk that is not in a securely protected environment, they must report this to the ICT Department so that the data can be encrypted with Council-approved encryption solutions.
- All employees, 3rd parties or contractors are responsible for the Council's assets, (particularly confidential data) that they use to carry out their function. Any suspicious activity or suspect breach in security must be immediately reported in accordance with the Council's Information Security Incident Management Policy.
- Ensure documents containing credit and debit cardholder data are securely locked away.

4.2 Credit Card Handling

4.2.1 Scope

This section provides the minimum mandatory requirements that need to be applied to all employees that handle or come across credit or debit cardholder data, in any format within the Council environment. Furthermore any third party that uses or accesses any of the Council's credit cardholder data, either physically or logically must also comply with this section. It is not the Council's intention to hold cardholder data, however, this section outlines what to do if such a situation arises.

4.2.2 Policy Statements

4.2.2.1 General

- Failure to protect card data can lead to large fines from banks, expensive investigations, expensive litigation, loss of reputation, and in the worst case scenario, withdrawal of the ability to take payment by credit cards; which would greatly hinder the Council's ability to conduct business.
- No staff should handle cardholder data unless you have explicit authorisation to do so.
- Cardholder data should only be handled in such a manner as is explicitly authorised by job roles.

4.2.2.2 Card Data Definitions and Requirements

- 'Credit Card Data' means most of the information on a Credit Card or Debit Card and includes the long 16 digit card number (Primary Account Number - PAN). It also includes the issue and expiry dates and the cardholder's name. The three digit security code on the back of the card is known as the Card Verification Value (CVV). The PAN must always be encrypted when electronically stored and the Cardholder data, if stored with the PAN must be protected.
- The CVV should be handled with great care and should never be written down or stored anywhere, whether on a piece of paper, a form, in a database, in a spreadsheet or any other electronic format, even if encrypted. The only exception to this is where you are taking a payment and need to store the CVV temporarily (pre-authorisation) whilst you arrange to take the payment. After the transaction has been authorised the CVV data must be destroyed immediately.
- If during the performance of your job you can see, by error or intention, a full card number when it is not required for you to do your job, please report this in accordance with the Council's Information Security Incident Management Policy. If, however, your job requires that you need access to the full credit card number and it is not mentioned in your job description, please report this to your line manager so that they can update your job description and confirm it with HR.

4.2.2.3 Card Data Handling Requirements

- Credit card data **MUST NOT** be routinely stored within the Council.
- Credit card data is classified as OFFICIAL-SENSITIVE, in accordance with the Council's Protective Marking Scheme (see the Information Management and Protection Policy). This means that if credit card data has to be stored for a particular reason then it must be protected. If it is stored in systems, it has to be encrypted. If it is stored on paper it must be locked away at all times unless in use. In the first instance, report any credit card number storage to the Council's ICT Manager.
- Do not store credit card data on laptops, desktop computers, file shares, memory sticks etc. unless these are on systems specifically approved for the storage of credit card data. If in doubt, do not store the data.
- Do not store credit card data in spreadsheets and other office documents, unless specifically required for your work, approved in writing by the Director of Resources and the document is encrypted to AES-256 bit standard.
- Any card data found or detected on Council systems must be reported in accordance with the Council's Information Security Incident Management Policy immediately upon discovery.

4.2.2.4 Printing of Documents Containing Card Data

There will be no cardholder data stored routinely within the Council and therefore there will be no printing of cardholder data. Should cardholder data exist, printing of it is expressly forbidden.

4.2.2.5 Handling Documents Containing Card Data

There are numerous cases where card data is legitimately stored on paper, be it a chargeback letter, a fraud document, an exceptions report, or when IT systems are unavailable and manual card payments are in operation. These data need to be retained only until the systems are back up again and card data can be processed electronically.

4.2.2.6 Vigilance and Awareness

- Credit card data can be inadvertently left on printers, fax machines, on a desk, on a screen, in a clear email (although this is against this Policy), in the 'trash' or 'recycle bin' file on a computer, in a temporary file, memory swap files etc.
- A good example of unusual locations to find credit card data is in call recordings. Occasionally telephone calls are recorded for quality and security purposes. These recorded calls can obviously contain the customer giving us their credit card details. To use these call recordings for training purposes the calls should be edited beforehand to remove any mention of a customer's credit or debit card details. So if you are listening to a call recording for training purposes, you should not hear a credit card number.

- If, however, as part of your job you are required to listen to complete calls (for example for real-time quality checking) this is acceptable. However, storing such calls for any length of time must be done securely within an approved storage system.
- Each employee or contractor is responsible to protect Council assets which include all forms of data. It is therefore important that, should you see any credit card data or other confidential data in a place that is insecure, inappropriate or where you do not expect to see it, even if your role includes the ability to work with credit card data you must:
 - a) secure the data, e.g. lock it in your desk;
 - b) report it to your team manager; and
 - c) report the incident in accordance with the Council's Information Security Incident Management Policy immediately.

4.2.2.7 PCI-DSS Data Retention

- Cardholder data must not be routinely stored on any Council system. Cardholder data that is approved to be stored temporarily must be deleted as soon as the reason for storing it has expired.
- Other data referring to the Cardholder Data Environment (CDE) will be treated as outlined below.

4.2.2.8 Payment Card Data

Payment card data will not be stored within the Council.

4.2.2.9 Revenue Protection Correspondence

This refers to all correspondence relating to charge-backs, revenue protection and fraud prevention. These will typically be paper copies and must be destroyed by cross-cut shredding once they have exceeded their retention period.

4.2.2.10 Information Systems and Physical Location Documentation

All documentation relating to Information Systems within the PCI-DSS CDE, including network diagrams, firewall access, system configuration, system passwords and backup documentation must be marked and treated as OFFICIAL-SENSITIVE and held securely with privileged access.

4.2.2.11 Audit Logs

There will be no cardholder data in the Council, therefore no audit logs fall in scope.

4.2.2.12 Cardholder Data Storage Locations

The Council does not store cardholder data.

4.2.2.13 Cardholder Data Disposal

The Council should not routinely hold any cardholder data.

However, if cardholder data exist on any system, the following actions must be taken where appropriate:

- All data must be securely disposed of when no longer required regardless of the media or application type on which it is stored.
- All hard copies of cardholder data must be manually destroyed as soon as it has reached the end of its retention period. A quarterly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner.
- The Council requires that all hardcopy materials are crosscut shredded, incinerated or pulped BEFORE they leave Council premises so they cannot be reconstructed.
- All cardholder information awaiting destruction must be held in lockable storage containers clearly marked "To Be Shredded" - access to these containers must be restricted.

4.3 Physical Security

4.3.1 Device Checking

Devices must be inspected at least monthly by staff to look for tampering (for example, addition of card skimmers to devices) or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). More information on how to inspect devices for tampering is given in Appendix 1.

Personnel will be trained to be aware of suspicious behaviour and to report tampering or substitution of devices.

Any tampering or suspicion that tampering has taken place must be reported immediately in accordance with the Information Security Incident Management Policy

4.3.2 Personnel Checking

- Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
- Do not install, replace, or return devices without verification.
- Be aware of suspicious behaviour around devices (for example, attempts by unknown persons to unplug or open devices).
- Report suspicious behaviour and indications of device tampering or substitution to the ICT Help-desk on Ext 165.

4.4 Acceptable Use

- The information system facilities of the Council are provided for business purposes and use of these facilities must be authorised in accordance with the IT Access Policy.
- It is mandatory for all users of systems and equipment within the Council's CDE to sign and adhere to the terms of the Transacting Officers' Protocol for Credit and Debit Card Data Management and the IT Access Policy.
- Employees and other users who deliberately breach the terms of this Policy will be subject to disciplinary action up to and including summary dismissal. Serious offenders are liable for prosecution under the Computer Misuse Act 1990.
- Every user is responsible for the proper use of the equipment they have been assigned and must comply with the Council's policies and all applicable laws.
- Users must ensure anti-virus is installed, up-to-date and operating on all Council devices, and report any failure of provision to the ICT Help Desk.
- It is prohibited to install and download any software on Council computers within the CDE, unless authorised by the ICT Manager.
- Any IT Systems equipment not belonging to the Council should not be installed on the Council network within the CDE, unless permitted, with the authorisation of the ICT Manager. Any such equipment must adhere to the standards within this document.

4.5 Responsibilities

All users within the CDE are responsible for:

1. Familiarising themselves with and adhering to the policies and procedures applicable to their area of responsibility;
2. Protecting Council equipment issued to them against unauthorised access and damage;
3. Using Council equipment for business purposes only;
4. Protecting Council and customer information against unauthorised access and loss;
5. Not disclosing their passwords or sharing user accounts;
6. Ensuring that Council IT systems and facilities (e.g. email or Internet) are used in accordance with the Council's policies;
7. Clearing desks of all sensitive material and logging off or locking workstations at the end of the day and when leaving their desk;
8. Not removing equipment, information or any other Council property from the organisation's premises without authorisation;
9. Not connecting personal equipment to Council networks within the CDE;

10. Not installing, copying or modifying any software on Council equipment without authorisation;
11. Immediately reporting security incidents in accordance with the Council's Information Security Incident Management Policy.

Responsibilities for carrying out specific information security duties will be defined in job descriptions where applicable.

5 Policy Compliance

5.1 Compliance Measurement

Compliance with policies is primarily enforced through process and standard documents that need to be developed by each business unit on how they perform their day to day activities in accordance with these policies.

5.2 Exceptions

Compliance with this Policy is mandatory.

5.3 Non-Compliance

Failure to follow this Policy will be considered as gross misconduct and may result in disciplinary action, up to and including summary dismissal.

5.4 Policy Review

This Policy will be reviewed at least annually by the IT Manager supported by the Corporate Information Governance Group (CIGG).

6 Related Standards, Policies, and Processes

This Policy is a part of West Lindsey District Council's Information Technology Security Policy set and must be read and applied in conjunction all relevant policies in the set.

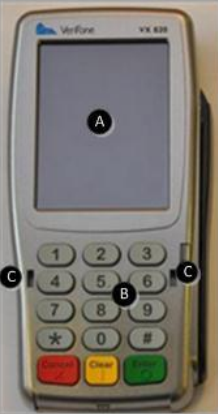




Appendix 1 - Detecting Evidence of Device Tampering

Device Details

Any devices not listed in this section are not MasterCard Payment Gateway Services P2PE supported devices.

Product Numbers: [Verifone Vx820] M282-701-C3-EUA-3 (Silver) M282-701-C3-EUB-3 (Black)

TNSPay – Pin Entry Device – Data Sheet

FRONT	REVERSE	BOTTOM	LEFT SIDE	RIGHT SIDE
				
<p>The top or front panel of the Vx820 PED is shown. This contains: A - colour touch screen B - keypad C - pin guard connector slots</p> <p>The facias are available in silver and black.</p>	<p>The back or reverse side panel of the Vx820 is shown. On this side the device labels can be found.</p> <p>The labels provide general information, specifically: A – Serial No. B – PTID C – MAC Address</p> <p>At the top end of the panel is a removable cover where the power and data cable is connected, and other connectors that can be used for mounting cradles.</p>	<p>The bottom of the Vx820 device is shown.</p> <p>Located at the bottom end of the device is the card reader for EMV/ICC cards (A).</p> <p>The MSR (magnetic stripe reader) is located on the right side of the unit (B).</p> <p>There are no identification or security markings/labels for these readers.</p>	<p>The left side of the Vx820 device is shown.</p> <p>It has no external marks or identifiers.</p> <p>The panel does contain a connector housing allowing other tethering options for enabling the unit to be physically fixed.</p>	<p>The right side of the Vx820 device is shown.</p> <p>The MSR (magnetic stripe reader) is located on this side of the unit.</p> <p>There are no additional identification marks, security identifiers, or connector options within this panel.</p>

Reverse Side Unique Identification Labels



- 1=General Information Label
 - Model Name
 - Power
 - Product Reference
- 2=S/N Unique Serial No*.
- 3=PTID (Physical terminal identifier)
- 4=MAC address
- 5=Cradle/Mount Connectors



- 1=Serial Number shown through the PED pack cover.

* Please note that if a PED pack option has been selected, the reverse side of the PED will be restricted and the PTID will not be visible. For the Tail Wind and Space Pole PED packs, only the serial number will be visible, an example is shown below:

Reverse Side Connectors



1=Data Connector Cable

Note: There is only once connection point in this device.

2=Security Seal

VeriFone's security seal covering a screw point only used at manufacture. The seal has an image of a VeriFone logo in silver.

3=SAM slots. 3 additional SAM slots.

Screw Positions



There are six screw positions on the back facia. Four are visible below the general information label. Two more are located under the back panel, one is covered by the VeriFone security seal.

Left Side Tether



A Secure Tether Adapter is located on the left facia of the device to allow secure tether options to be attached to the device.

POI Weights

The Vx820 weighs 0.68lb or 308g.

Source: http://global.verifone.com/media/540007/2667-vf-vx820_data-sheet_web.pdf

Inspecting the Device

Deployed payment devices in the merchant's environment must be inspected periodically. This is to detect evidence of tampering, substitution or modification.

The pictures above show the P2PE devices in their manufacturer issues state. Merchants can use this information to conduct visual and physical inspections to validate the integrity of the devices.

