London Borough of Enfield

Payment Card Industry – Data Security Standard Policy
# CONTENTS

1. Introduction........................................................................................................ 3  
2. Aims and Objectives .......................................................................................... 3  
3. PCI DSS applicability to the Council ............................................................... 3  
4. Roles and responsibilities .................................................................................. 4  
5. Definitions.......................................................................................................... 4  
6. Approach to PCI DSS compliance ..................................................................... 4  
7. Compliance Actions ........................................................................................... 5  
8. Security Process and Standards reference to SAQ ............................................ 5  
8.1  Do Not Use Vendor Supplied Defaults for System Password and other Security Parameters .......................................................... 6  
8.2  Protect Cardholder Data .................................................................................. 7  
8.3  Maintain a Vulnerability Management Program ............................................. 9  
8.6  Develop and Maintain Secure Systems and Applications ................................. 9  
8.7  Restrict Access to Cardholder Data by Business Need to Know ..................... 10  
8.8  Identify and Authenticate Access to System Components .............................. 10  
8.9  Restrict Physical Access to Cardholder Data ................................................ 11  
8.10 Regularly Monitor and Test Networks .......................................................... 12  
8.11 Regularly Test Security Systems and Processes ............................................ 13  
8.12 Maintain a Security Policy that Addresses Information Security for All Personnel ...................................................................................................................... 14  
9. Security Breaches............................................................................................. 17  
10. Corporate Card Payment Systems .................................................................... 17  
11. Card Payment Terminals (PDQ machines) ...................................................... 18  
12. Storage of Card Details .................................................................................... 19  
13. Data Retention and Disposal ............................................................................ 19  
14. Electronic Transfer of Data .............................................................................. 19  
15. Point of Sale (PoS) Card Services ................................................................... 19  
16. Refunds ............................................................................................................ 20  
17. Contacts............................................................................................................ 20  
18. Definitions ........................................................................................................ 20  
Appendix A: Terminal Security Procedures .......................................................... 20
1. Introduction

Payment Card Industry Data Security Standards (PCI-DSS) is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data.

It consists of a number of steps and security best practices that help to ensure the secure processing of sensitive data throughout the Council, and the Council has an obligation to protect confidential cardholder information through compliance with PCI DSS.

Failure to comply with these regulations could result in cardholder data becoming compromised, data security breaches, substantial fines, severe reputational damage and/or the loss of income, and potentially the revoking of the Council’s authority to accept card payments.

This policy applies to anyone performing Council duties or providing Council services facilitating card payments. It applies to Councillors; other organisations conducting Council business; employees; contractual third parties and agents of the Council.

Anyone who uses the Council’s systems should be made aware of and be expected to comply with this policy and need to understand that the PCI DSS requirements relevant to protecting cardholder information:

A serious breach of this policy could be regarded as gross misconduct and may lead to dismissal and / or criminal action being taken.

Compliance with this policy is part of your employment contract. All incidents will be investigated, and action may be taken under the Council’s formal disciplinary procedure. A serious breach of this policy could be regarded as gross misconduct and may lead to dismissal and / or criminal action being taken. In the most serious cases, this could be dismissal without prior warning.

2. Aims and Objectives

The objective of this policy is to ensure that all card processing activities of the Council will comply with the PCI-DSS industry standard. No activity or technology may obstruct compliance with the PCI DSS.

This policy aims to set out the requirements of the PCI DSS in respect of the transmission, processing and storage of cardholder data, and the key responsibilities in connection with the achievement and maintenance of compliance with PCI DSS. It applies to all individuals and systems within the Council that come into contact with cardholder data, whether this is electronic or paper based.

3. PCI DSS applicability to the Council

The Council does not store payment card data but does process and transmit card payments which are subsequently handled by external ‘service providers’ who are each certified as being PCI DSS compliant.

The Council is a ‘Level 3 Merchant’ (processing between 20,000 and 1,000,000 transactions per annum) which means that certification to the Standard requires the completion of an annual Self-Assessment Questionnaire (SAQ) to demonstrate
This is a CONTROLLED document. Any printed copy must be checked against the current electronic version prior to use.

4. Roles and responsibilities

The recognised user groups are:

1. Staff processing card payments – this could be face to face payments, or payments taken over the phone, and processing card refunds, and includes contractors or anyone else used to process card payments directly for the Council. These staff must understand and comply with the policy.
2. Council Managers and Team Leaders – must ensure that their staff understand the policy and are aware of their obligation to comply with it.
3. Finance Manager – responsible for ensuring that the Council meets the requirements of the PCI DSS and submission of the annual Self-Assessment Questionnaire (SAQ) to prove compliance.
4. PCI Compliance Officer – report to the Finance Manager and must ensure that an up to date list of card payment devices is maintained, relevant card payment security training is carried out and that staff comply with this policy. This role is covered by the IT Security Manager
5. ICT Services – must manage IT Services and Infrastructure in accordance with the requirements of PCI DSS.

Services must comply with this policy to minimise the risk to both customers and the Council. Failure to comply will render the Council liable for fines and may also result in preventing card transactions from being processed.

5. Definitions

PCI DSS is concerned with account data for debit and credit cards. Account data is made up of cardholder data and sensitive authentication data (also known as sensitive information), and there are specific rules around the use, storage and transmission of these two types of data.

Cardholder data refers to the card number across the centre of the card (otherwise known as the Primary Account Number, or PAN), the cardholder name, the expiry date and the service code (also known as the security code).

The primary account number is the defining factor for cardholder data. If the cardholder name, service code, and/or expiry date are stored, processed or transmitted with the PAN, they must be protected in accordance with the PCI DSS requirements. Storage of cardholder data is permitted but must always be protected with strong encryption. If the PAN is not stored, this requirement is lifted.

Sensitive information is security-related information. This includes (but is not limited to) card validation codes, full track data (from the magnetic stripe or equivalent on a chip), PINs and PIN blocks. This information is used to authenticate cardholders and/or authorise payment card transactions.

Under no circumstances can sensitive information be stored in any form after authorisation.

6. Approach to PCI DSS compliance
Full compliance to the highest level of requirements is very resource intensive. Where possible, we will look to use systems and processes that reduce the level of compliance required. For this reason it is important to consult the Finance Officer before starting any process re-design, and particularly any procurement process, involving card payments. It is also important to think about the visibility of cardholder data during the processing of the payment, so the PCI Compliance Officer should also be consulted regarding office moves.

The requirements set out below are based on the full PCI DSS requirements. Implementing systems and processes that reduce the compliance level required will mean that the requirement could be not applicable to all channels. However, they are included in the policy document so that we have an agreed process to follow should any channel be identified as being of the highest compliance level.

7. Compliance Actions

Other actions will be taken to encourage compliance, namely:

1. A third party company is under contract to monitor Council compliance with PCI DSS through quarterly network scans.
2. The Council submits an annual Self-Assessment Questionnaire (SAQ) to prove compliancy.
3. 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.
4. Ad hoc checks will take place to ensure employees are maintaining PCI-DSS security procedures.
5. Annual compliancy confirmation will be sought from all staff processing electronic card payments.

8. Security Process and Standards reference to SAQ

8.1 Build and maintain a Secure network and system

To protect sensitive or confidential data, it is critical to design and maintain a secure network infrastructure where this data can be processed and transmitted. The following policies cover the network infrastructure (hardware such as firewalls, routers, and switches) as well as requirements for the secure configuration of all system components (network hardware, servers, workstations, etc.).

8.1.1 Install and Maintain a Firewall Configuration to protect card holder data

Firewalls are devices that control computer traffic allowed between LBE networks (internal) and untrusted networks (external). A firewall examines all network traffic and blocks those transmissions that do not meet LBE specified security criteria. All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee email access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network. Other system components may provide firewall functionality, as long as they meet the minimum requirements for firewalls as defined in this requirement. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of requirement 1.
8.1.2 Prohibit Direct Public Access between the Internet and any System Component in the Cardholder Data Environment

LBE will prohibit direct public access between the Internet and any system component in the cardholder data environment by doing the following:

- A firewall is required between the cardholder data network and the Internet. (PCI-DSS Requirement 1.3.3)
- Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. (PCI-DSS Requirement 1.3.5)
- Use a firewall that implements stateful inspection, also known as dynamic packet filtering. (That is, only “established” connections are allowed into the network.) (PCI-DSS Requirement 1.3.6)

8.1.3 Restrict Connections between Untrusted Network Segments and the Cardholder Data Environment

LBE will restrict connections from untrusted network segments to system components within the cardholder data by doing the following:

- Maintain firewall and router configuration standards documentation1. (PCI-DSS Requirement 1.2)
- Firewall rules must limit all inbound and outbound traffic to/from the cardholder data network to only that which is necessary for business. (PCI-DSS Requirement 1.2.1).
- When wireless networking is used, a firewall is required between any wireless network and the cardholder data environment. Firewall rules must prohibit insecure traffic and restrict traffic from the wireless segment to only that which is necessary for business. (PCI-DSS Requirement 1.2.3)

8.2 Do Not Use Vendor Supplied Defaults for System Password and other Security Parameters

System components used in sensitive networks often will come with default vendor settings (usernames, passwords, configuration settings, etc.). LBE’s general policy is to always change vendor-supplied defaults for system passwords or other security parameters before systems are installed in the secure network environment (cardholder data network).

8.2.1 Change Vendor Supplied Defaults
- All vendor-supplied defaults must be changed on all system components before being used in the cardholder data network. (e.g., passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts, etc.). (PCI-DSS Requirement 2.1, 2.2.d).

8.2.2 System Hardening and Standard Configuration of Devices
- Documented system configuration standards1 must:
  - Be consistent with either SANS, ISO, NIST, CIS, or similar security industry standards and address PCI configuration requirements (e.g., password requirements, log settings, File Integrity Monitoring, Anti-virus software, etc.). (PCI DSS Requirement 2.2)

---

1 See the System Hardening and Configuration Standards document.
• Be developed that address all system components and address all known security vulnerabilities for systems used in the Cardholder Data Environment. (PCI DSS Requirement 2.2.a)
• Be updated as new vulnerabilities are identified. (See Section 6.1) (PCI DSS Requirement 2.2.b)
• Be applied when new systems used in the Cardholder Data Environment are configured and before systems are placed into production. (PCI DSS Requirement 2.2.c)
• Include only one primary function is implemented per server. If virtualization technologies are used, each virtual system or virtual component must have only one primary function. (PCI DSS Requirement 2.1.d, 2.2.1)
• Include unnecessary or insecure services, daemons, protocols are not enabled or are justified and documented as to the appropriate use of the service. (PCI DSS Requirement 2.2.d, 2.2.2)
• Include security parameter settings for all devices in the card network. (PCI DSS Requirement 2.2.d)
• Include additional security features implemented for insecure services, protocols or daemons. (PCI DSS Requirement 2.2.d, 2.2.3)
• Include all required functionality. These functions must support secure configuration, and only documented functionality may be present on systems in the card network. (PCI DSS Requirement 2.2.d, 2.2.4)
• Include the removal of all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers from system components in the Cardholder Data Environment and document all enabled functions for each system. (PCI DSS Requirement 2.2.d, 2.2.5)

8.2.3 Use Secure Protocols for Non-Console Access
Strong cryptography must be used for any non-console or web-based management interface used for administration of systems or system components. (Use technologies such as SSH, VPN, or the latest secure versions of TLS for web-based management and another non-console administrative access.) (PCI-DSS Requirement 2.3).

8.2.4 Security Policies and Operational Procedures Documentation
Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties. (PCI-DSS Requirement 2.5)

8.3 Protect Cardholder Data
Cardholder data (PAN and sensitive authentication data) must not be stored electronically. Credit card data has many sensitive components, including the Primary Account Number (PAN), magnetic stripe authentication data (Track1, Track2), Card Verification Code (CVC), and the Personal Identification Number (PIN), etc.

8.3.1 Storage of Sensitive Credit Card Authentication Data
• Never store Sensitive Authentication Data (Track, CVC, and PIN) after an authorization event has taken place (even if encrypted). (PCI DSS Requirement 3.2.d)
• All sensitive authentication data must be deleted or rendered unrecoverable upon completion of the authorization process. (PCI DSS Requirement 3.2.c)
• Never store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere) in any database, log file, debug file, etc. after any type of card authorization event. (PCI DSS Requirement 3.2.1)
• Never store the Card Validation Code (CVC) data (3- or 4-digit number located on the back or front of the credit card) in any database, log file, and debug file, etc. after any type of card authorization event. (PCI DSS Requirement 3.2.2)
• Never store the Personal Identification Number (PIN) data (includes actual PIN number or Encrypted PIN block obtained during a debit card transaction from the PIN Entry Device) in any database, log file, debug file, etc. after any type of card authorization event. (PCI DSS Requirement 3.2.3).

8.4 Encrypt Transmission of Cardholder Data across Open, Public Networks
Cardholder data must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

8.4.1 Transmission of Card Data over Public Networks
• Strong encryption algorithms and protocols (i.e., TLS, IPSEC, SSH) must be used whenever cardholder data is transmitted or received over open, public networks.
  The following controls must be part of the LBE data transmission policies: (PCI DSS Requirement 4.1.a)
  • Only trusted keys or certificates will be accepted. (PCI DSS Requirement 4.1.b)
  • The data transmission protocol must be implemented to use only secure protocol configurations, and must not support insecure versions or configurations (e.g., use the latest secure TLS and SSH versions only). (PCI DSS Requirement 4.1.c)
  • The encryption strength is appropriate for the encryption methodology in use. (PCI DSS Requirement 4.1.d)
  • For TLS implementations, TLS must be enabled whenever cardholder data is transmitted or received. (PCI DSS Requirement 4.1.e)
  • If SSL or early TLS is used on a POS POI terminal, documentation must be created detailing how it was verified that the terminal is not susceptible to any known exploits for SSL or early versions of TLS. Documentation must include evidence (vendor documentation, system/network configuration details, etc.). (PCI DSS Requirement 4.1.f)
  • If SSL or early TLS is used anywhere but a POS POI terminal, a risk mitigation and migration plan must be created, which includes the following: (PCI DSS Requirement 4.1.g)
    • Description of how it is used, including what data is being transmitted, the types and number of systems that use and/or support SSL or early TLS and the type of environment.
    • The risk assessment results, including the risk reduction controls that are in place.
    • A process of how new vulnerabilities associated with SSL and early TLS are monitored.
    • A description of change control processes that are in place to ensure no new environments are created which utilize SSL and/or early TLS.
• An overview of the migration project plan that includes a migration completion date no later than June 30th, 2018.

8.4.2 Transmission of Card Data via End User Messaging Technologies
It is prohibited to transmit cardholder data via end-user messaging technologies (e.g., e-mail, instant messaging, etc.). (PCI-DSS Requirement 4.2).

8.5 Maintain a Vulnerability Management Program
System components within the cardholder data network(PCIDSS DMZ) must be part of an active vulnerability maintenance program. This program will control the existence of malicious software (e.g., anti-virus software) and provide policies covering development efforts and system or software updates/upgrades such that security is maintained.

8.5.1 Deploy anti-virus software to protect systems
- Anti-virus software must be deployed on all systems in the card network that are commonly affected by malicious software. This includes personal computers, servers, etc. that are attached to the Cardholder Data Environment. (PCI DSS Requirement 5.1)
- Anti-virus programs must be capable of detecting, removing, and protecting against all known types of malicious software (adware, spyware, etc.). (PCI DSS Requirement 5.1.1)
- For systems considered not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats to confirm whether such systems continue not to require anti-virus software. (PCI DSS Requirement 5.1.2)

8.5.2 Ensure that all anti-virus mechanisms are current
- All anti-virus software and its associated definition files must be kept up-to-date at all times. (PCI DSS Requirement 5.2.a)
- All anti-virus software must be actively running, configured to perform automatic updates, and set to run periodic scans. (PCI DSS Requirement 5.2.b)
- Anti-virus software must be capable of generating audit logs and audit logs must be retained for one year. (PCI DSS Requirement 5.2.c)

8.5.3 Ensure that all anti-virus mechanisms are actively running
- All anti-virus software installations and configurations must be actively running at all times. (PCI DSS Requirement 5.3)
- Anti-virus configurations do not allow users to disable or alter the software unless specifically authorized by management on a case-by-case basis for a limited time. (PCI DSS Requirement 5.3)

8.6 Develop and Maintain Secure Systems and Applications
Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches that must be installed by the entities that manage the systems. All systems must have all appropriate software patches to protect against the exploitation and compromise of cardholder data by malicious individuals and malicious software.
8.6.1 Vulnerability risk ranking process
- System administrators are to subscribe to outside sources for security vulnerability information and system configuration standards are to be reviewed and updated as new vulnerability information might dictate. Outside sources might include National Vulnerability Database, SecurityFocus, A/V companies, SANS, CIS, Secunia, Microsoft, etc. (PCI DSS Requirement 6.1)
- When any vulnerability (or potential vulnerability) is found using the documented vulnerability discovery and risk ranking process, it must be evaluated and assigned a ranking based on the risk level. At a minimum, the highest risk vulnerabilities should be assigned a “High” risk ranking. (PCI DSS Requirement 6.1)

8.6.2 Regularly update systems and software
- All system components and software must have the latest vendor-supplied security patches installed. (PCI DSS Requirement 6.2.a)
- All critical system and software patches must be installed within 30 days of vendor release. (PCI DSS Requirement 6.2.b)

8.7 Restrict Access to Cardholder Data by Business Need to Know
Systems and processes must be in place to limit access to critical data and systems based on an individuals need to know and according to job responsibilities. “Need to know” is when access rights are granted to the least amount of data and privileges needed to perform a job.

8.7.1 Restrict Access to Cardholder Data and Systems in Cardholder Data Environment
- Access to cardholder data and system components must be restricted to only those individuals whose job requires such access. (PCI DSS Requirement 7.1)
- Restrict access to privileged user IDs to the least privileges necessary to perform job responsibilities and assigned to only those roles that specifically require the privileged access. (PCI DSS Requirement 7.1.2)
- Access assigned to individual personnel is based on their job classification and function. (PCI DSS Requirement 7.1.3)

8.8 Identify and Authenticate Access to System Components
It is critical to assign a unique identification (ID) to each person with access to critical systems or software. This ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

8.8.1 Vendor Access
- Manage IDs used by vendors to access, support, or maintain system components via remote access, ensuring that they are only enabled for the time period needed, disabled when not in use and they are monitored by LBE employees during use. (PCI DSS Requirement 8.1.5a-b)

8.8.2 User Authentication Methods
- In addition to assigning a unique user ID, access to systems in the card network requires the use of at least one of the following: (PCI DSS Requirement 8.2)

---

2 See the Vulnerability Discovery and Risk Ranking Process document.
• Something you know, like a password or passphrase
• Something you have, like a token device or smart card
• Something you are, like a Biometric

- Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. (PCI DSS Requirement 8.2.1)
- Verify user identity before modifying any authentication credential (for example, performing password resets, provisioning new tokens, or generating new keys.) (PCI DSS Requirement 8.2.2)
- Passwords or phrases must meet the following: (PCI DSS Requirement 8.2.3)
  o Require a minimum length of at least seven characters
  o Contain both numeric and alphabetic characters
- Change user passwords/passphrases at least every 90 days. (PCI DSS Requirement 8.2.4)
- Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/phrases they have used. (PCI DSS Requirement 8.2.5)
- Set all first time use and reset passwords to a unique value for each user and require immediate change after first use. (PCI DSS Requirement 8.2.6)

8.8.3 Multi-factor Authentication
- Incorporate multi-factor authentication for all non-console administrative access to the cardholder data environment. Multi-factor authentication is also required for all remote access originating from outside the cardholder data environment by personnel, including users and administrators and all third parties, including vendor access for support or maintenance. (PCI DSS Requirement 8.3)

8.8.4 Group or Shared Accounts and Passwords
Do not use group, shared, or generic accounts or passwords or other authentication methods as follows: (PCI DSS Requirement 8.5.)
- Generic user IDs are disabled or removed.
- Shared user IDs do not exist for system administration and other critical functions.
- Shared and generic user IDs are not used to administer any system components.

8.8.5 Security Policies and Operational Procedures Documentation
- Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties. (PCI DSS Requirement 8.8)

8.9 Restrict Physical Access to Cardholder Data
Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies and should be appropriately restricted.

If sensitive cardholder data is ever discovered or received, management must be notified and it shall be immediately destroyed, redacted, or truncated following the information in section 9.8 of this policy. (PCI-DSS Requirement 9.8)

8.9.1 Limits and Monitor Physical Access to Systems
Restrict access to network jacks by implementing physical and/or logical controls. (PCI-DSS Requirement 9.1.2)
8.9.9 Protection from Tampering and Substitution

- Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. (PCI-DSS Requirement 9.9)
- Maintain an up to date list of devices that includes the following: (PCI-DSS Requirement 9.9.1/See Payment Terminal Device Review Log in Table 2)
  - Make and model of the device
  - Location of the device
  - Device Serial number or other method of unique identification.
- Periodically inspect device surfaces to detect 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). (PCI-DSS Requirement 9.9.2)
- Provide training for personnel to be aware of attempted tampering or replacement of devices.
- Training should include the following: (PCI-DSS Requirement 9.9.3)
  - 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 appropriate personnel (for example, to a manager or security officer).

8.10 Regularly Monitor and Test Networks

Important components of overall system security are the regular testing of networks for exposed vulnerabilities and the continuous monitoring of security indicators (logs, system events, etc.). The following policies address system monitoring and vulnerability testing. Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs. Detailed monitoring procedures should be developed and documented to meet the following policies.

8.10.2 Generation of Audit Trails

- Implement automated audit trails for all system components to capture the following events: (PCI DSS Requirement 10.2)
  - All actions taken by any individual with root or administrative privileges. (PCI DSS Requirement 10.2.2)
  - Invalid logical access attempts. (PCI DSS Requirement 10.2.4)
  - Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges. (PCI DSS Requirement 10.2.5)

8.10.3 Audit Trail Entries

- Record at least the following audit trail entries for all system components for each event: (PCI DSS Requirement 10.3)
  - User Identification. (PCI DSS Requirement 10.3.1)
  - Type of event. (PCI DSS Requirement 10.3.2)
  - Date and Time. (PCI DSS Requirement 10.3.3)
  - Success or failure indication. (PCI DSS Requirement 10.3.4)
• Origination of event. (PCI DSS Requirement 10.3.5)
• Identity or name of affected data, system component, or resource. (PCI DSS Requirement 10.3.6)

8.10.6 Log Review
• Review logs and security events for all system components to identify anomalies or suspicious activity by performing the following: (PCI DSS Requirement 10.6)
• Review the following at least daily: (PCI DSS Requirement 10.6.1)
  • All security events.
  • Logs of all system components that store, process, or transmit CHD and/or SAD, or that could affect the security of CHD and/or SAD.
  • Logs of all critical system components.
  • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).
• Review logs of all other system components periodically based on the organization’s policies and risk management strategy, as determined by the organization’s annual risk assessment.3 (PCI DSS Requirement 10.6.2)
• Follow up exceptions and anomalies identified during the review process. (PCI DSS Requirement 10.6.3)

8.10.7 Audit Trail History
Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (e.g., online, archived, or restorable from backup). (PCI DSS Requirement 10.7)

8.11 Regularly Test Security Systems and Processes
Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software must be tested frequently to ensure security controls continue to reflect a changing environment. Detailed testing procedures4 should be developed and documented to meet the following policies.

8.11.2 Vulnerability Assessment Scans
• Internal and external vulnerability assessment scans must be performed at least quarterly and after any significant change in the cardholder data environment (e.g., changes in firewall rules, or upgrades to products within the environment, etc.). (PCI DSS Requirement 11.2, 11.2.3)
• Internal vulnerability scans must be: (PCI DSS Requirement 11.2.1.a-c)
  • Performed quarterly.
  • Be performed by a qualified internal resource with organizational independence or a qualified external third party.
  • Have a process to include a rescan until all “high-risk” vulnerabilities (as defined in PCI DSS Requirement 6.1) are resolved. (PCI DSS Requirement 11.2.3.b)
• External vulnerability scans must (PCI DSS Requirement 11.2.2.a-c)
  • Be performed quarterly.

---

3 See the Risk Assessment Process document.
4 See the Operating Procedures document.
• Be performed by an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC) with rescans until passing scans are achieved.
• Contain no vulnerabilities that are scored 4.0 or higher by the CVSS.
• Run on all external IP addresses that could be used to gain access to the cardholder data environment. (PCI DSS Requirement 11.2)
• Ensure that results of each quarter’s internal and external vulnerability assessments are to be documented and retained for review. (PCI DSS Requirement 11.2)

8.11.3 Penetration Testing
• If segmentation is used to isolate the Cardholder Data Environment from other networks, a segmentation test is required to confirm all methods of segmentation are effective in isolating the Cardholder Data Environment from out-of-scope systems or networks. These tests must be documented and performed at least annually and after any changes to segmentation controls or methods. (PCI DSS Requirement 11.3.4)

8.11.5 Change Detection
• Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. (PCI DSS Requirement 11.5)
• A process is in place describing how to respond to alerts generated by the change-detection mechanism. (PCI DSS Requirement 11.5.1)

8.12 Maintain a Security Policy that Addresses Information Security for All Personnel
A strong security policy sets the security tone for LBE and informs employees and vendors what is expected of them. All employees and vendors should be aware of the sensitivity of data and their responsibilities for protecting it.
8.12.1 Publish, Distribute, and Update the Information Security Policy
• LBE requires that the most recent version of the information security policy be published and disseminated to all relevant system users (including vendors, contractors, and business partners). (PCI DSS Requirement 12.1)
• The LBE information security policy must be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. (PCI DSS Requirement 12.1.1)

8.12.4 Assign Information Security Responsibilities and Train Employees
• The LBE’s information security policy and procedures apply to all employees (full, part-time, or work study employees), contractors, and individuals providing services for LBE and could affect security of cardholder information. (PCI DSS Requirement 12.4)

8.12.5 Assign Information Security Management
• The overall responsibility of information security at LBE falls under the office of <Role or Department>. (PCI DSS Requirement 12.5)
• Specifically, the following responsibilities must be assigned: (see form in Appendix A)
• Establishing detailed documentation of security incident response and escalation procedures and distributing these procedures. (PCI DSS Requirement 12.5.3)

8.12.6 Security Awareness Program
• A formal security awareness program must exist and participation is required for all employees working within the cardholder data environment. (PCI DSS Requirement 12.6.a)

8.12.8 Policies for Sharing Data with Service Providers
• In order to conform to industry best practices, it is required that due diligence is performed before engaging with new service providers and is monitored for current service providers that store, process, or transmit cardholder data on LBE’s behalf. Service providers, which could affect the security of cardholder account data, are also in-scope of this policy.
  • LBE shall maintain a documented list of all applicable service providers in use. (PCI DSS Requirement 12.8.1)
  • A written agreement with all applicable service providers is required and must include an acknowledgement of the service providers’ responsibility for securing all cardholder data they receive from or on behalf of LBE, or to the extent that they could affect the security of a cardholder data environment (PCI DSS Requirement 12.8.2). In addition, the service provider must agree to provide compliance validation evidence on an annual basis. (PCI DSS Requirement 12.8.4). Prior to engaging with an applicable service provider, a thorough due diligence process should be followed. (PCI DSS Requirement 12.8.3)
  • LBE shall annually review evidence provided by applicable service providers demonstrating their continuing PCI DSS compliance. (PCI DSS Requirement 12.8.4)
  • LBE shall maintain a list of which PCI DSS requirements are managed by each service provider, and which are managed by LBE. (PCI DSS Requirement 12.8.5)

8.12.10 Incident Response Plan Policies
Incidents or suspected incidents regarding the security of the cardholder data environment or cardholder data itself must be handled quickly and in a controlled, coordinated and specific manner. An incident response plan must be developed and followed in the event of a breach or suspected breach. The following policies specifically address the LBE incident response plan.
  • LBE must maintain a documented incident response plan (IRP) and be prepared to respond immediately to a system breach. (PCI DSS Requirement 12.10)
  • The IRP must clearly define roles and responsibilities for response team members. (PCI DSS Requirement 12.10.1)
- The IRP must define communication strategies to be used in the event of a compromise including notification of payment brands. (PCI DSS Requirement 12.10.1)
- The IRP must define specific incident response procedures to be followed. (PCI DSS Requirement 12.10.1)
- The IRP must document business recovery and continuity procedures. (PCI DSS Requirement 12.10.1)
- The IRP must detail all data back-up processes. (PCI DSS Requirement 12.10.1)
- The IRP must contain an analysis of all legal requirements for reporting compromises of sensitive data (for example, California Bill 1386 which requires notification of affected consumers in the event of an actual or suspected compromise of California resident’s data). (PCI DSS Requirement 12.10.1)
- The IRP must address coverage and responses for all critical system components. (PCI DSS Requirement 12.10.1)
- The IRP must include or reference the specific incident response procedures from the payment brands. (PCI DSS Requirement 12.10.1)
9. Security Breaches

In the event of there being a security breach of data, staff must report the breach to the ICT Service Desk who will follow our Incident Handling Procedure. The Finance Manager must be involved in the investigation.

The PCI Compliance Officer must then contact the customer and/or card provider to ensure that card processing is discontinued immediately if this is appropriate. Additionally if there is a risk to Rights and Freedoms of individuals there is a requirement to report any breach to the Data Protection regulator – please see the Data Protection Policy.

10. Corporate Card Payment Systems

The Council has a corporate electronic card payments system which allows various types of income to be paid using a number of means as listed below:

- Online
- Telephone
- Automated Telephone Line
- Kiosk (card and cash)

**Online Processing**

In the first instance customers should make payment for goods and services online using the Pay Online link on the Enfield website, however only certain payments are set up to pay using this method. This is the preferred method and best practice for taking payments.

On completion of a successful payment the online system being used will automatically generate an email payment confirmation to the customer. This is the only Finance confirmation document that will be received by the customer for the payment.

If a customer’s payment has been unsuccessful or declined, the customer in the first instance should contact their card provider. The most common reason for a declined transaction is the card provider suspecting the transaction may be fraudulent.

If a customer faces difficulty in making a payment then they can contact the Customer Service Centre where an agent will answer queries and can take the payment over the telephone if necessary.

**Telephone Processing**

Various payments can be taken over the telephone by either a Customer Service Centre agent or specific service officer. Card details must never be written down by any member of staff for a future payment attempt. For all card details which are processed through the corporate payments system, no card details are retained by the authority.

There is no internal Council access to full card details as this information is not stored within the Council's IT network.
11. Card Payment Terminals (PDQ machines)

There are specific services that use PDQ terminals and not the Corporate Payments System. Where these terminals are used the following procedures apply.

Customer Present with a Card

When the customer is present the card should be processed through the PDQ machine according to the machine instructions.

If the transaction is successfully processed, the merchant copy should be stored securely (see Storage of Card Details) and the customer copy given to the customer. If the transaction is declined, the customer should be advised immediately. The option of paying with a different card should be offered. The customer copy stating that the payment was declined should be given to the customer and the merchant copy should be stored securely (see Storage of Card Details).

By Telephone

Where card details are provided during a telephone call, these must be processed directly into the PDQ terminal at that time and must not be written down or noted anywhere.

When card details are being provided in a telephone call these must not be repeated back to the customer in such a way as to be audible to third parties.

If it is not possible to submit the card details immediately then a call back must be requested or offered.

Services using such devices must take ownership of their use and adhere to the requirements listed below in Appendix A, Terminal Security Procedures.

Card Details Received in Writing

Some customers may provide their card payment information in writing for processing i.e. by fax, in a letter, email or by booking form. Customers should be deterred from providing the information in this manner as it is not secure. There is no guarantee that these details have not been intercepted prior to being received by the Council.

When details have been received by this method they must be processed immediately upon receipt.

Once the payment has been successfully authorised, the original document showing the full card details must be crosscut shredded.

If the details have been received by email, then the email must be deleted from the Inbox and the Deleted mail folder. If the email requires a response, the card information provided should not be contained within the reply. Note that this does not immediately remove the data which will remain available for a period, hence this should be avoided if possible.
In a situation where it is not possible to process the transaction immediately then the details must be stored in a secure environment such as a locked drawer or cabinet. This is only to be actioned in exceptional circumstances.

For PDQ records, if the transaction is successfully processed, the merchant copy should be stored until transaction reconciliation complete.

If the transaction is declined, the customer should be advised immediately. The option of paying with a different card should be offered. The customer copy stating that the payment was declined should be sent to the customer and the merchant copy should be stored within the till drawer or cash box for the duration of the working day. When storing merchant copy receipts these must be treated as a confidential document and should be marked accordingly.

12. Storage of Card Details

Storage of card details on computers in any format (e.g. email, Access databases, Excel spreadsheets, USB memory sticks) breaches the regulations. Staff are specifically forbidden from storing data electronically.

If this occurs the result could be large monetary fines from Visa and MasterCard. This is because there is risk of fraudsters obtaining card details by hacking into computers or storage media which stores cardholder information.

Merchant copies of PDQ receipts must be destroyed once transaction reconciliation complete. All other paper records containing sensitive information must be destroyed immediately after authorisation.

13. Data Retention and Disposal

Services are responsible for complying with the council’s Retention Schedule which can be found on Enfield Eye.

Services retaining non-sensitive card data must carry out a review, at least quarterly, to remove data that exceeds requirements defined in the data retention policy.

Retained data on paper should be securely disposed of by cross-cut shredding when no longer required.

14. Electronic Transfer of Data

It is strictly prohibited to transfer card data electronically both internally or externally to Enfield Council. This includes the use of end user messaging technologies.

15. Point of Sale (PoS) Card Services

All devices in use must comply with PCI standards.

All devices are included in the inventory for Enfield Council which contains key data identified by the standard.

Devices must be periodically inspected to detect tampering or substitution.
Staff using such devices must be trained to be aware of attempted tampering or replacement of devices.

Services using such devices must take ownership of their use and adhere to the requirements listed below in Appendix A, Terminal Security Procedures.

16. Refunds

Corporate Electronic Payments

Refunds can only be processed back to the originating card if:
(a) the card is still valid and
(b) if the payment was made either online or via the telephone where customer information has been completed (but not automated payment line or Kiosk card transactions).

The refund must be approved by the responsible Service Head via email then forwarded to the nominated person.

The corporate system is then accessed and the refund is processed back to the source card from which the original transaction was authorised. It is possible to process part refunds where necessary but the refund cannot exceed the original amount.

Other Payment Methods

Refunds for other payment methods have to be processed by completing Payment Request Form which is processed and paid via the Finance system. This is because the original payment does not capture the cardholder’s details to facilitate a refund.

17. Contacts

If you have any questions about the details in this policy, or have difficulty complying with any part of it, please contact the Finance Manager or the ICT Service Desk

Related Information
General information about PCI-DSS can be found at https://www.pcisecuritystandards.org/pci_security/why_security_matters

18. Definitions

PCI DSS The Payment Card Industry Data Security Standards
PSP Payment Service Providers, e.g. Capita, Sage Pay, Spektrix
CDE Cardholder Data Environment
SAQ Self-Assessment Questionnaire
PDQ Process Data Quickly or Pretty Damn Quick
CVV Card Verification Value (3 digit code on back of card)
CVC Card Verification Code (3 digit code on back of card)
PoS Payment locations utilising PDQ card devices

Appendix A: Terminal Security Procedures
These procedures apply to all payment terminals and PIN-entry devices, including:
- Branch terminals (standalone PDQs).
- Portable terminals (mobile PDQs).
- Connected Pin Entry Devices (chip&pin)

**Acceptable Use**
Terminals may only be used for taking customer payments for verified payments.
Terminals may only be used by authorised personnel.

**Daily Checks – Anti-Tampering**
To ensure terminals are not tampered with, at start of day:
Perform routine visual inspections of every device, looking for potential signs of tampering. Also keep track of any operational difficulties that begin happening on a regular basis. Some examples of things to look for include:
- Damaged or altered tamper seals
- Missing manufacturer labels
- Missing screws or screws with damaged heads
- Incorrect keyboard overlays
- External wires
- Holes in the device housing
- An electronic serial number that does not match the number printed on the label on the bottom of the device
- A high number of mag-stripe read failures or debit card declines
- Difficulty inserting a chip and PIN card into the EMV slot

If tampering or overlooking of the terminal is suspected, it must not be used.
All details must be reported to the ICT Service Desk.