Payment Card Industry Data Security Standards Policy

1. Introduction

As an organisation that takes payments by debit and credit cards, we must comply with a set of standards to ensure the security of the card information. The standards are known as the Payment Card Industry Data Security Standards (PCI DSS), and they apply to organisations around the world. They are set out by the Payment Card Industry Security Standards Council (PCI SSC), and this policy sets out how Canterbury City Council and its staff will comply with these standards. Failure by the council to comply with the standards could result in regular and large fines and also no longer being permitted to process card payments.

It is important that all card processing activities are conducted in accordance with this policy and no activity may be conducted, nor technology employed, that might obstruct compliance with any part of this policy.

There are 12 broad areas, grouped by 6 headings, covered by the security standards, some of which affect how ICT, system suppliers or system administrators will set up the council's systems and others that impact directly on staff throughout the council who take card payments from customers. The 12 areas, and the 6 grouped headings, are:

Build and maintain a secure network and systems:

- Install and maintain a firewall configuration to protect cardholder data;
- Do not use vendor-supplied defaults for system passwords and other security parameters;

Protect cardholder data:

- Protect stored cardholder data;
- Encrypt transmission of cardholder data across open, public networks;

Maintain a vulnerability management program:

- Protect all systems against malware and regularly update anti-virus software or programs;
- Develop and maintain secure systems and applications;

Implement strong access control measures:

- Restrict access to cardholder data by business need to know;
- Identify and authenticate access to system components;
- Restrict physical access to cardholder data;

Regularly monitor and test networks:

- Track and monitor all access to network resources and cardholder data;
- Regularly test security systems and processes;

Maintain an information security policy:

- Maintain a policy that addresses information security for all personnel.

This policy lays down the guidelines by which we will achieve compliance against these standards. Where possible, risk will be managed and requirements on the council will be reduced by the use of appropriate payment channels or alternative suppliers. However, an assessment will be made for each payment channel individually.

2. Statement of Applicability

PCI DSS compliance for each authority is the responsibility of the PCI Compliance Officer.

The policy applies primarily to any staff member, but also extends to contractors of the council, suppliers, hosts of external systems and anyone else who is involved in processing card payments, handling of till receipts, or with responsibility for payment systems or networks, even on a temporary basis. However, not all parts of the policy apply to all staff, so the requirements are broken down into the different user groups. Recognised user groups are:

- 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.
- Staff who have interactions with card processing companies and/or banks for the purposes of financial reconciliation, including contractors or anyone else employed by the council to carry out this work.
- System administrators. This covers any system that has a card payment element, including till systems in use at various outlets within the district.
- ICT staff, with regard to systems connected to, or using, the council network.
- Suppliers of hosted systems have the same responsibilities as ICT for any systems that are hosted externally and not on the council network.
- PCI Compliance Officer.
- All staff. There are a few requirements that all staff should be aware of, as it affects the handling of till receipts, or considerations when visitors are in the office.

Staff within these groups will need to work together to achieve and maintain PCI DSS compliance. Technical advice will be provided by the most appropriate people, but any changes or introduction of new systems or processes should ultimately be signed off by the PCI Compliance Officer, as the system will need to comply with PCI DSS requirements.

If any person is found to have breached this policy, they will be subject to the council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of offenders.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or the PCI Compliance Officer.

Identified Roles

It is recognised that each council has different job titles, so the following table is provided to help staff identify who they should contact, and also so that individual staff are aware of their responsibilities.

	Canterbury	Dover	Thanet
PCI Compliance Officer	Claire Stanbury		
ICT	EKS ICT Team	EKS ICT Team	EKS ICT Team
Corporate Information Officer	Matthew Archer		
Corporate Governance and Risk Officer	Sue Wallis		
Customer Service Manager	Jo Read	Jo Read	Jo Read
Office Services Manager	Alexis Jobson		

3. 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.

What is Cardholder 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 the PAN must always be rendered unreadable.

What is Sensitive Information?

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.

4. 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 PCI Compliance 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.

In order to remove the requirement for the highest levels of control, we need to ensure that systems are not stored on our network, and that payments are not processed on devices that are connected to our network unless they have validated point to point encryption.

5. Requirements

5.1 Firewall

Why is this important?

Often, seemingly insignificant paths to and from external networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

A firewall examines network traffic and blocks the transmissions that do not meet the security criteria.

Responsibilities of PCI Compliance Officer

5.1.1 To ensure that policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.

Responsibilities of ICT

5.1.2 To ensure that policies and operational procedures are in place for managing firewalls, and that these are complied with.

5.1.3 To maintain firewall and router configuration standards in line with up-to-date PCI DSS requirements, and to review the rule sets at least every six months.

5.1.4 To ensure the firewall configuration will restrict connections between untrusted networks and any system components in the cardholder data environment. Inbound and outbound traffic will be restricted to just what is necessary

5.1.5 To prohibit direct public access between the internet and any system component in the cardholder data environment.

5.1.6 If we have any environments that require the highest level of control, to install firewall software on any corporate mobile devices provided that connect to the internet when outside the network, and which are also used to access the network.

Responsibilities of all staff

5.1.7 To ensure that any devices that connect to the internet when outside the network are not connected to any networked equipment without being scanned by ICT, unless approved firewall and anti-virus software has been installed.

5.2 System passwords and security parameters

Why is this important?

Malicious individuals often use vendor default passwords and other default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information. Default passwords and settings must be changed in order to protect against this threat.

Responsibilities of PCI Compliance Officer

5.2.1 To ensure that policies and procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.

5.2.2 To ensure that inventories of system components exist for all payment areas and that procedures are in place for these to be checked daily.

5.2.3 To maintain a record of systems that are not up to date, and the risk assessments completed, reviewing these at least six-monthly to understand the current risk and to review if the issue still exists.

Responsibilities of ICT

5.2.4 To ensure that all systems installed on the network have default passwords changed before installation on the network.

5.2.5 To develop configuration standards for all system components to address all known security vulnerabilities and that are consistent with industry accepted ICT risk management standards.

5.2.6 When implementing upgrades or new software into the cardholder environment, to seek advice from the software vendor about relevant security vulnerabilities, and how the software should be configured in order to fix or minimise the vulnerabilities where feasible.

5.2.7 To complete a risk assessment if it is not feasible to install latest patches; which must be sent to the PCI Compliance Officer.

Responsibilities of system administrators

5.2.8 To ensure that all systems installed on the network have all default passwords changed, working with ICT support if necessary.

5.2.9 To maintain an inventory of system components for payment systems/point of sale terminals.

5.2.10 To ensure that processes are in place for daily checks of system components, comparing equipment in place to that shown in the inventory, and that these are carried out each day.

Responsibilities of staff on point of sales terminals

5.2.11 To check at the start of each day that the components shown in the inventory are in place and have not been compromised, completing the daily sign off sheet to confirm that all components have been checked and are in order.

5.3 Protecting stored cardholder data

Why is this important?

Cardholder data must be protected to prevent theft or misuse of this information, which could lead to fraudulent transactions being processed. This includes any information held electronically or on paper records, and information being sent between staff. By ensuring that the amount of data held is minimal, or masked so that it cannot be read, the risk is reduced.

Responsibilities of PCI Compliance Officer

5.3.1 To ensure that policies and procedures for protecting cardholder data are documented, in use, and known to all affected parties.

Responsibilities of ICT

5.3.2 To ensure that no logs, history or trace files store sensitive information or unmasked cardholder data.

5.3.3 To apply processes that actively search for sensitive information or unmasked cardholder data every six months.

Responsibilities of system administrators

5.3.4 To ensure that payment systems never store sensitive information, including the card security code, after a payment has been authorised.

5.3.5 To ensure that the full PAN is masked when displayed on screens, receipts, printouts etc. The first six and last four digits are the maximum number of digits that can be displayed.

5.3.6 To ensure that the maximum amount of information recorded and stored is the card number (rendered unreadable), expiry date and name. This applies to printed till receipts, as well as electronic information stored.

Responsibilities of managers

5.3.7 To ensure that departmental retention schedules include cardholder data, whether in electronic systems or on till receipts, to ensure this is not stored any longer than necessary, and is destroyed securely. This information should only be stored for as long as is required for business, legal or regulatory purposes. Advice can be sought from the PCI Compliance Officer or the Corporate Information Officer if necessary.

5.3.8 To seek approval from the PCI Compliance Officer if data is to be held for longer than 18 months.

Responsibilities of staff processing card payments

5.3.9 To ensure that cardholder data, including the card security code, is never written down, and that it is never stored unencrypted after a payment has been authorised.

5.3.10 No cardholder data should ever be taken or stored off council premises.

5.3.11 To ensure that card numbers and security codes are not repeated in full back to customers in an area that can be overheard by others.

5.4 Encrypting transmissions of cardholder data

Why is this important?

Sensitive information must be encrypted during transmission to protect it from malicious individuals able to intercept the transmission. Misconfigured networks and vulnerabilities in security protocols continue to be targeted by malicious individuals to gain access to cardholder data and sensitive information.

Responsibilities of PCI Compliance Officer

5.4.1 To ensure that policies and procedures for encrypting transmissions are documented, in use, and known to all affected parties.

Responsibilities of ICT

5.4.2 To ensure that cardholder data is encrypted using strong cryptography and security protocols when being transmitted over open, public networks.

Responsibilities of staff processing card payments

5.4.3 To ensure that card numbers are never sent in emails, instant messaging, chat, or any other end-user messaging. This includes card numbers captured as part of a screen dump.

5.5 Anti-virus software and protection against malware

Why is this important?

Malicious software can enter the network during normal business activities, including email and use of the internet. This software can then be used to gain access to our systems and data in various ways. Anti-virus software must therefore be installed on all systems at risk of being affected, and on all hardware such as laptops and PCs.

General

The requirements within section 5.5 only apply if we have environments that require the highest levels of control. However, the installation, updating and use of anti-virus software would still be considered best practice and as such these requirements should be met as far as is possible.

Responsibilities of PCI Compliance Officer

5.2.12 To ensure that policies and procedures for protecting systems against malware are documented, in use, and known to all affected parties.

Responsibilities of ICT

5.2.13 To ensure that anti-virus software is installed on all systems at risk of being affected by malicious software. The software must be capable of detecting, removing and protecting against all known types of malicious software.

5.2.14 To ensure that anti-virus software in use is kept current and actively running, performs periodic scans and generates audit logs.

5.2.15 To ensure that anti-virus software cannot be disabled or altered by users, unless specifically authorised by management for a limited time period.

Responsibilities of staff processing card payments

5.2.16 To ensure that anti-virus software installed on hardware is actively running.

4.2 Develop and maintain secure systems

Why is this important?

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided patches, which must be installed promptly, to protect against the exploitation and compromise of cardholder data by malicious individuals.

General

5.6.1 As much as possible, we will limit exposure to these risks by using industry standard, PCI DSS compliant certified software and systems, rather than creating bespoke systems.

5.6.2 Most of the requirements within section 5.6 only apply if we have environments that require the highest levels of control. All responsibilities of the PCI Compliance Officer need to be met regardless, as do points 5.6.7, 5.6.9, 5.6.12, 5.6.13 and 5.6.15 to 5.6.17.

Responsibilities of the PCI Compliance Officer

5.6.3 To ensure that policies and procedures for developing and maintaining secure systems are documented, in place, and known to all affected parties.

5.6.4 To ensure that vulnerabilities identified through PCI compliance testing are addressed as they are discovered.

5.6.5 To provide testing card details to departments for testing payment systems and mechanisms.

5.6.6 To ensure that Open Web Application Security Project (OWASP) guidelines cover the requirements of PCI DSS.

Responsibilities of ICT

5.6.7 To employ a process to identify security vulnerabilities, and to assign a risk ranking to any newly discovered vulnerabilities.

5.6.8 To inform the PCI Compliance Officer and the Corporate Governance and Risk Officer once a vulnerability has been identified, detailing the risk identified and to discuss plans for remediation.

5.6.9 To work with system administrators to ensure that system components and software are kept up to date with security patches. Critical security patches should be implemented within 30 days if possible. Where this is not possible, the PCI Compliance Officer and the Corporate Governance and Risk Officer should be informed, so that the risk can be recorded and action monitored.

5.6.10 To work with system administrators to ensure that vulnerabilities identified through PCI compliance testing are addressed as they are discovered.

5.6.11 To ensure that change control processes are followed for all changes to system components, ensuring that live card numbers are not used for testing or development purposes.

5.6.12 To ensure that any software or web applications developed internally are compliant with Open Web Application Security Project (OWASP). When applications are developed which require a link to a payment mechanism, it must be discussed with the PCI Compliance Officer and be compliant with PCI DSS standards.

5.6.13 If applications are developed internally, ensure that developers use secure coding techniques, and understand how sensitive information will be handled in transmission, storage and memory.

5.6.14 To ensure that an automated technical solution that detects and prevents web-based attacks (for example, a web application firewall) is maintained in front of any public-facing web applications that have contact with the cardholder data environment, or review public-facing web applications via application vulnerability security assessment tools annually and after any changes.

Responsibilities of system administrators

5.6.15 To employ a process to identify security vulnerabilities, and to assign a risk ranking to any newly discovered vulnerabilities.

5.6.16 To inform the PCI Compliance Officer and the Corporate Governance and Risk Officer once a vulnerability has been identified, detailing the risk identified and to discuss plans for remediation.

5.6.17 To work with ICT to ensure that system components and software are kept up to date with security patches. Critical security patches should be implemented within 30 days if possible. Where this is not possible, the PCI Compliance Officer and the Corporate Governance and Risk Officer should be informed, so that the risk can be recorded and action monitored.

5.6.18 To work with ICT to ensure that vulnerabilities identified through PCI compliance testing are addressed as they are discovered.

5.6.19 To ensure that change control processes are followed for all changes to system components, ensuring that live card numbers are not used for testing or development purposes.

5.7 Controlled access

Why is this important?

To protect cardholder data and sensitive information, access to it should be limited to only those people with a need to access it.

Responsibilities of PCI Compliance Officer

5.7.1 To ensure that policies and procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.

Responsibilities of system administrators

5.7.2 To only grant access to system components that deal with cardholder data, and to cardholder data itself, to those that need access for the purposes of their job.

5.7.3 To ensure that access to a system is only granted once authorised by the line manager, and once the user has acknowledged that they have read and understood this policy, and will comply with its content.

5.7.4 To maintain an audit trail of access authorisation and acknowledgement of the policy.

5.7.5 To ensure that payment systems automatically deny access to the parts of the system that process cardholder data, so that access has to be expressly given.

Responsibilities of staff processing card payments

5.7.6 To ensure that cardholder data is never copied, moved or stored onto local hard drives or removable media, such as memory sticks.

5.8 Identifying and authenticating system access

Why is this important?

All users of payment systems should be identifiable, so that any discrepancies can be investigated and traced. The identification should ideally be by means of a unique computer log in, but can also be achieved by other means, such as the use of cameras overlooking cashier terminals (although care should be taken that the cameras do not record cardholder data being entered).

Minimum password requirements

5.8.1 The following are the minimum password requirements as set out by the PCI DSS requirements.

- Minimum length of at least 7 characters.
- Contain both alphabetic and numeric characters.
- Must be changed at least once every 90 days.
- Must not be the same as any of the last 4 passwords.

Responsibilities of PCI Compliance Officer

5.8.2 To ensure that policies and procedures for identification and authentication are documented, in use, and known to all affected parties.

Responsibilities of ICT

5.8.3 To ensure that multi-factor authentication is in place for remote access to the network by employees, administrators and third parties.

5.8.4 To ensure that vendor accounts are managed so that they are only enabled when authorised, and that they have access appropriate to their role. Access will be monitored.

5.8.5 To ensure that computers and other devices issued by ICT are set to lock after 15 continuous minutes of inactivity.

Responsibilities of system administrators

5.8.6 To ensure that unique IDs are provided to individual users, unless other identification means exist, such as cameras recording the cashiering area.

5.8.7 To ensure that password security settings for all systems that process cardholder data comply with the minimum password requirements set out in 5.8.1 above.

5.8.8 To immediately revoke the user IDs for any users no longer requiring access.

5.8.9 To remove or disable inactive user accounts at least every 90 days (or ensure that the payment system carries this out automatically).

5.8.10 To ensure that users are locked out after no more than 6 unsuccessful attempts of logging into the system, with a minimum lockout time of 30 minutes, unless cleared by an administrator.

5.8.11 To ensure that user identity is verified before modifying any authentication credentials such as passwords.

5.8.12 To use unique passwords for first time use and upon reset of accounts, and to ensure these are set to change immediately after first use.

Responsibilities of staff processing card payments

5.8.13 To only log in to the Council's approved payment systems using only the ID provided by the system administrator.

5.8.14 To ensure that personal login details are kept safe and **never** shared with others, and that passwords are changed if there has been a risk of passwords being shared or known by others.

5.8.15 To ensure that passwords used comply with the minimum password requirements set out in 5.8.1 above.

5.8.16 To lock the computer whenever leaving the office, or lock other devices when not in use.

5.8.17 To not amend the lockout time on any device beyond that set by ICT when issued.

5.9 Physical access

Why is this important?

Any physical access to data, or systems that house cardholder data, provides the opportunity for individuals to access devices or data and to remove information, and should be appropriately restricted.

This applies to electronic data, but also any paper that may contain cardholder data, such as till receipts.

Responsibilities of the PCI Compliance Officer

5.9.1 To ensure that policies and procedures for restricting physical access are documented, in use, and known to all affected parties.

5.9.2 To ensure that appropriate controls are in place for physical areas where cardholder data is processed, to prevent reading of cardholder data by unauthorised persons.

Responsibilities of ICT

5.9.3 To ensure that electronic media is stored securely, and when removed this is performed in line with agreed procedures.

5.9.4 To store media backups in a secure location, and to review the location's security annually.

5.9.5 To ensure that cardholder data is rendered unrecoverable on any electronic media that is no longer required.

Responsibilities of system administrators

5.9.6 To protect devices that capture payment card data from tampering and substitution.

5.9.7 To maintain an up-to-date list of card payment devices, including the following:

- Make and model of device;
- Location of device;
- Serial number or other unique identification information;
- Device expiry date;
- Any substitution of device due to authorised replacement or repair.

5.9.8 To periodically inspect devices for tampering and substitution.

5.9.9 To train personnel to be aware of attempted tampering or replacement of devices.

Responsibilities of the Customer Service Manager

5.9.10 To ensure that all physical areas where cardholder data is processed are laid out and access is controlled in appropriate ways, to prevent reading of cardholder data by unauthorised persons.

5.9.11 To ensure that main reception maintain a log of visitors, including details of the visitor's name, firm represented if applicable, the person they are visiting and the date of the visit.

Responsibilities of the Office Services Manager

5.9.12 To ensure that arrangements exist for the secure destruction of paper based confidential information in such a way that the data cannot be reconstructed.

Responsibility of service managers

5.9.13 To ensure that remote sites have appropriate visitor logs and procedures in place, ensuring that visitors are recorded and can be identified whilst on site.

5.9.14 To ensure that all records, whether paper or electronic, which contain cardholder data are stored and transported securely, preferably by using corporate methods for the destruction of confidential information.

5.9.15 To ensure that records are clearly marked so that they can be identified as confidential before being transported. Where records are sent from one building to another, this must be done in a secure way that can be tracked, such as using the standard council courier service.

Responsibilities of all staff

5.9.16 To follow the standard council guidelines with regard to visitors, ensuring that they have signed in at reception, are authorised before entering areas where cardholder data is processed or maintained, that they wear the visitor badge issued at reception, and that the badge is given up at the end of their visit.

5.9.17 To ensure that paper records being sent to another area are sent in a non-transparent sealed envelope or wallet, and are not loose within a clear messenger bag or wallet.

5.9.18 To store till receipts or other cardholder data records in line with local policies, ensuring that they are secure at all times.

5.9.19 To ensure that till receipts or other records containing cardholder data are disposed of using the council's confidential waste bins, and that they are kept no longer than necessary, in line with departmental retention schedules.

5.10 Monitoring access to data

Why is this important?

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 allows thorough tracking, alerting and analysis if something should go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

General

5.10.1 The requirements within section 5.10 only apply if we have environments that require the highest levels of control. Where possible we will implement systems and processes that require lower levels of control. However, should systems be implemented that require the highest level, then the requirements within this section will need to be complied with.

Responsibilities of PCI Compliance Officer

5.10.2 To ensure that policies and procedures for monitoring access to network resources and cardholder data are documented, in use, and known to all affected parties.

Responsibilities of ICT

5.10.3 To maintain system logs that link all access to system components to individual users.

5.10.4 To use appropriate software to search for cardholder data on a quarterly basis.

5.10.5 Where cardholder data exists, to maintain logs that are able to reconstruct:

- access to cardholder data;
- actions taken when logged in with administrator privileges;
- access to audit trails;
- invalid login attempts;
- use of authentication mechanisms;
- initialisation, stopping, or pausing of audit logs;
- creation and deletion of system level objects.

5.10.6 To ensure that logs record the identity of the user, date and time of events, and whether or not events were successful.

5.10.7 To ensure that audit logs maintained are secure against alteration, and can only be viewed by those with a job related need.

5.10.8 To review logs and security events to identify anomalies or suspicious activity on a daily basis for all security events, system components that store, process or transmit cardholder data or sensitive information, all critical system component logs and logs of all server and system components that perform security functions.

5.10.9 To review logs of all other systems on an alert basis to identify anomalies or suspicious activity.

5.10.10 To ensure that logs are routinely backed up and maintained for 1 year.

5.10.11 To ensure that all system clocks and times are synchronised.

5.11 Testing security systems and processes

Why is this important?

Vulnerabilities are being discovered continually, and being introduced by new software. System components, processes, and custom software should be tested

frequently to ensure security controls continue to reflect a changing environment.

General

5.11.1 Most of the requirements within section 5.11 only apply if we have environments that require the highest levels of control. However, we will need to perform quarterly internal and external network scans regardless of the other controls required. All other requirements will only be needed where a system is implemented that requires the highest level of control.

Responsibilities of PCI Compliance Officer

5.11.2 To ensure that policies and procedures for security monitoring and testing are documented, in use, and known to all affected parties.

Responsibilities of ICT

5.11.3 To test quarterly for the presence of wireless access points, taking appropriate action to close any unauthorised points identified.

5.11.4 To maintain an inventory of authorised wireless access points.

5.11.5 To perform quarterly internal and external network scans to identify any PCI vulnerabilities.

5.11.6 To perform internal and external network scans to identify any PCI vulnerabilities after any significant changes in the network, and to rescan as needed until all high risk vulnerabilities are resolved. If an upgrade or modification could allow access to cardholder data, or affect the security of the cardholder data environment, this would be considered significant.

5.11.7 To undertake internal and external penetration testing annually, with extra scans taking place after any significant changes in infrastructure or relevant applications, and to rescan as needed until all high risk vulnerabilities are resolved.

5.12 Maintaining a policy for ourselves and contractors

Why is this important?

All personnel should be aware of the sensitivity of data, and their responsibilities for protecting it. A strong security policy sets the tone for the whole entity and informs personnel of what is expected of them.

When choosing suppliers to work with for payments, it's also necessary to ensure they are aware of the responsibility of protecting such data, and that their systems and processes are PCI DSS compliant.

Responsibilities of the PCI Compliance Officer

5.12.1 To maintain and review the PCI DSS policy annually, taking into account up-to-date PCI guidance.

5.12.2 To ensure that an annual audit of PCI compliance is carried out to ensure continued compliance with the standards, and look at newly identified risks.

5.12.3 To ensure that a risk assessment is carried out upon significant changes to the environment, such as the introduction of a new payment channel.

5.12.4 To maintain a list of third party companies who provide card payment services on behalf of the council, and ensure that these companies are also compliant with PCI standards.

5.12.5 To obtain an annual statement from suppliers providing card payment services, recognising their responsibility for the security of cardholder data they store, process or transmit on behalf of the council.

5.12.6 To ensure the maintenance of an incident response plan, ensuring that it contains all requirements as set out by the PCI council. As a minimum, this includes:

- Roles, responsibilities and communication strategies in the event of a compromise, including notification to payment brands.
- Specific incident response procedures.
- Business recovery and continuity procedures.
- Data backup processes.
- Analysis of legal requirements for reporting compromises.
- Coverage and responses of all critical system components.
- Reference or inclusion of incident response procedures from the payment brands.

5.12.7 To ensure that the Information Security Policy complies with up to date PCI DSS requirements.

5.12.8 To implement a formal security awareness program to make all personnel aware of the importance of cardholder data security, educating staff annually and upon hire.

Responsibilities of ICT

5.12.9 To assist in the annual audit of PCI compliance, providing information on how the networks and systems meet up-to-date PCI requirements.

Responsibilities of system administrators

5.12.10 To assist in the annual audit of PCI compliance, providing information as requested to prove that systems are still compliant with up-to-date PCI requirements.

5.12.11 If appointing a new company to handle card payments on our behalf, to ensure their PCI status is checked and taken into account before they are appointed. Guidance can be sought from the PCI Compliance Officer.

5.12.12 To ensure that any new contracts awarded for payment solutions require adherence to PCI DSS by the service provider and include acknowledgement of responsibility for the security of cardholder data.

Responsibilities of staff processing card payments

5.12.13 To ensure they are familiar with their responsibilities under this policy, and that they are being carried out fully.

Responsibilities of all staff

5.12.14 To ensure that any concern regarding a security risk or abuse of the system or policy is reported to the PCI Compliance Officer. If the matter is particularly sensitive it can be raised under the Council's whistle blowing policy.

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed;

- Councils' disciplinary procedure.
- Breach of contract.
- Member code of conduct.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Office.

Document Control		
Title/Version	-	CIGG Password Policy 1.0
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
22/10/2015	Will Causton	1.0	Initial Version
19/01/2016	Hannah Lynch	1.1	Format Changes
23/09/2016	CIGG	1.2	Final Review