Payment Card Industry - Data Security Standard (PCI-DSS)

Stanford & Green

Security Policy

Version 6

8 January 2026

Document Management

Those to whom this Policy applies are responsible for familiarising themselves periodically with the latest version and for complying with Policy requirements at all times.

Version Number	Date	Circulation	Changes	Reviewed
1.0	03/02/17	All Staff / IT manager	First issue	AM
1.1	6 January 2021	All Staff / IT Manager	Second Issue	MS
1.2	6 January 2023	All Staff / IT Manager	Third Issue	MS
1.3	16 January 2024	All Staff – IT Manager	No changes	MS
1.4	10 January 2025	All Staff – IT Manager	No changes	MS
1.5	8 January 2026	All Staff – IT Manager	No Changes	MS

1. Introduction

This policy sets out the requirements which are necessary to protect the security of all credit and debit card payments received and processed by Stanford & Green which are governed by the Payment Card Industry Data Security Standard (PCI-DSS). Compliance with PCI-DSS is mandatory for any company or organisation which stores, processes, or transmits payment cardholder data. Failure to comply with these requirements could result in the company being fined and no longer permitted to process card payments.

The policy applies primarily to staff associated with the Cardholder Data Environment (CDE)[1] but extends to anyone else who processes card payments, even on a temporary basis.

It will be reviewed annually as a minimum and updated where necessary in accordance with the PCI-DSS Standard to reflect changes to business objectives, risk environment, changes to the CDE and in-scope systems and signed off by an independent Internal Security Assessor (ISA) or commissioned Qualified Security Assessor (QSA).[2]

This document was approved in February 2017 by the Managing Director and Finance Director. It is recognised that there are specific processes and Stanford & Green's Standards need to be developed in support of the Policy.

2. PCI-DSS Applicability to Stanford & Green

Stanford & Green does not store or transmit payment card data but does process card payments which are subsequently handled by external 'service providers 'who are -DSS compliant.

Stanford & Green is a 'Level3Merchant'[3]which means that certification to the Standard requires the completion of an annual self-assessment questionnaire (SAQ) to demonstrate compliance.

3. Summary of Requirements and Applicability to Stanford & Green

The PCI-DSS defines the minimum criteria required for those processing card payments to become and remain compliant. This section provides a summary of the prescriptive controls as defined in Appendix 1.

The PCI-DSS Security Policy is supported by Stanford & Green's PCI-DSS specific documentation comprising:

Network Security Standard;

a. Systems Security Standard;

b. Operational Security Standard;

c. Access Control Standard;

d. Training Standard;

e. Incident Response Plan; and, Finance Procedures.

These documents outline the specific requirements in each respective area to enable Stanford & Green to comply and maintain compliance with the PCI-DSS.

1. Only those members of the Stanford & Green who are officially employed or engaged in a role associated with the CDE are permitted to access systems and technologies which form part of the CDE, and then only in accordance with their specific responsibilities and permissions associated with that role.

2. All changes to the CDE will be managed and controlled according to the Stanford & Green management process.

3. Devices which are capable of storing or transmitting unencrypted data must not be connected to any system or device which forms part of the CDE, either physically or logically. Where appropriate PCs will be configured to prevent connectivity of such devices.

4. All requests for technical support for components within the CDE must be recorded with Stanford & Green's Management, to provide full audit reports of incidents, faults and resolution activities.

5. Staff processing card payments must fully comply with the 'Processing of Credit and Debit Card Payments', and adhere to Stanford & Green's Information Security Policies and the scope of the CDE

6. Computers and technologies used for or in association with the CDE are not to be used for any purpose other than official Stanford & Green business.

7. Privately-owned computers and other equipment (including mobile telephones, laptop computers and tablets) must not be used for the processing, storage or transmission of any cardholder data associated with any aspect of Stanford & Green's business.

8. No components, including individual Virtual Terminals (VTs), PIN Entry Devices (PEDs), web payment servers and tills, are to be added to or removed from the CDE without the explicit consent of Stanford & Green's Finance Director.

9. Payment card data is not to be processed or stored on any computer or transmitted via any network without having first obtained the express permission of the Finance Director.

The authority of Stanford & Green's Director, service being commissioned which will involve the processing of credit and debit card payments and all new payment applications must be PCI-PA DSS compliant.

10. Any computer and other equipment which forms part of CDE must not be connected to the wireless network without the prior written consent of the IT manager.

12. The IP addresses of computers and other equipment which forms part of the CDE must not be changed without the prior written consent of the Managing Director/IT manager.

Virtual Terminals (VTs) and Web Payment Servers

13. No software is to be installed on VTs and servers except for software which is used for official Stanford & Green business and which is installed by official IT Support staff who are authorised to work on systems which form part of the CDE, or by recognised third parties who are associated with systems within the CDE.

14. Monthly checks will be undertaken of all VTs to ensure that automated anti-virus software and security patching mechanisms have been effective and that the protection remains current.

15. Security patches for operating systems and applications will be applied to systems which are in scope and part of DSS compliance. These will be applied within 28 days of release. Anti-virus software will be maintained on all such systems.

16. Support of VTs and servers will only be carried out by authorised computer technicians who are familiar with the specific configuration and the environment in which they are located.

17. Only authorised technicians will be permitted to remotely connect to VTs and servers and only approved software and methods will be permitted for this purpose.

Virtual Terminal Operations Areas

22. Cameras, mobile telephones (incorporating cameras) and visual, and audio recording devices must not be used in areas accommodating VTs.

23. All staff VTs are to be physically checked on each occasion prior to being booted up to ensure that there is nothing which looks untoward or suspicious, such as a device connected to a USB port or spurious cables. Anything which appears suspicious must be reported immediately to the IT manager.

PIN Entry Devices (PEDs)

24. Only PEDs which are listed on the *https://www.pcisecuritystandards.org/* website as being an approved PIN Transaction Security Device (PCI PTS) will be used by Stanford & Green.

Appendix 1 Applicable PCI-DSS Policy Requirements

The PCI-DSS defines the minimum criteria required for those processing card payments to become and remain compliant. This section outlines the minimum requirement which needs to be implemented in order for a Level 3 Merchant to be compliant with the Standard in accordance with the requirements of SAQ C.

	Policy Undertaking
PCI-DSS Req.	***Requirement 1*** ***Install and maintain a firewall configuration to protect cardholder data***
1.2	Firewall and router configurations shall restrict connections between un-trusted networks and any system components in the CDE.
1.2.1	Inbound and outbound traffic shall to be restricted to that which is necessary for the CDE.
1.2.3	Perimeter firewalls must be installed between any wireless networks and the CDE, and configured to deny or control (as applicable) any traffic from the wireless environment into the CDE.
1.3	Direct public access between the Internet and any system component in the CDE is prohibited.
1.3.1	A DMZ must be implemented to limit inbound traffic to only system components that provide authorised publicly accessible services, protocols, and ports.
1.3.3	Direct connections inbound or outbound for traffic between the Internet and the CDE is not allowed.
1.3.5	Unauthorised outbound traffic from the CDE to the Internet is not allowed.
1.3.6	Dynamic packet filtering must be implemented.
PCI-DSS Req.	***Requirement 2*** ***Do not use vendor-supplied defaults for system passwords and other security parameters***
2.1	Vendor-supplied defaults must be changed before installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.
2.1.1	The wireless vendor defaults for wireless environments connected to the CDE must be changed before connectivity, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.
2.2.2	Only necessary and secure services, protocols and daemons as required for the function of the system are to be enabled.
2.3	All non-console administrative access must be encrypted using strong cryptography. Technologies such as SSH, VPN, or SSL/TLS must be used for web-based management and other non-console administrative access.
PCI-DSS Req.	***Requirement 3*** ***Protect stored cardholder data***
3.3	The Primary Account Number (PAN) will be masked when displayed.
PCI-DSS Req.	***Requirement 4*** ***Encrypt transmission of cardholder data across open, public networks***
4.1	Strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH) must be used to safeguard sensitive cardholder data during transmission over open, public networks.
4.1.1	Wireless networks transmitting cardholder data or connected to the CDE, must use industry best practices to implement strong encryption for authentication and transmission.
4.2	PANs must not be sent by unprotected end-user messaging.

PCI-DSS Req.	***Requirement 5*** ***Use and regularly update anti-virus software or programs***
5.1	Anti-virus software must be deployed on all systems commonly affected by malicious software.
5.1.1	Ensure that all utilised anti-virus programs used are capable of detecting, removing, and protecting against known types of malicious software.
5.2	All anti-virus mechanisms must be current, actively running, and generating audit logs.
PCI-DSS Req.	***Requirement 6*** ***Develop and maintain secure systems and applications***
6.1	All system components and software are to be protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Critical security patches must be installed within one month of release.
PCI-DSS Req.	***Requirement 7*** ***Restrict access to cardholder data by business need to know***
7.1	Access to system components and cardholder data must be limited to only those individuals whose job requires such access. Access limitations must include the following:
7.1.1	Access rights to privileged user IDs will be restricted to the least privileges necessary to perform job responsibilities.
7.1.2	Assignment of privileges must be based on individual personnel’ function.
PCI-DSS Req.	***Requirement 8*** ***Assign a unique ID to each person with computer access***
8.3	Where applicable, two-factor authentication will be used for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication).
8.5.6	Accounts used by vendors for remote access must only be enabled when needed and must be monitored when in use.
PCI-DSS Req.	***Requirement 9*** ***Restrict physical access to cardholder data***
9.6	All cardholder data must be physically secure.
9.7	Strict control is to be maintained over the internal and external distribution of any kind of media.
9.7.1	Media must be classified so the sensitivity of the data can be determined.
9.7.2	The media must be sent by secure courier or by another delivery method that can be accurately tracked.
9.8	Management must approve any and all media that is moved from a secured area.
9.9	Strict control must be maintained over the storage and accessibility of media.
9.10	All media must be destroyed when it is no longer needed for business or legal reasons as follows:
9.10.1	Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.
PCI-DSS Req.	***Requirement 10*** ***Track and monitor all access to network resources and cardholder data***

10.0	There are no controls in section 10 as part of SAQC.
PCI-DSS Req.	***Requirement 11*** ***Regularly test security systems and processes***
11.1	Tests are to be undertaken on a quarterly basis for the presence of wireless access points and to detect any unauthorised wireless access points.
11.2	Both internal and external network vulnerability scans must be performed at least quarterly[5] and after any significant change to systems which form part of the CDE or which support payment card transactions.
11.2.1	Perform quarterly internal vulnerability scans.
11.2.2	Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).
11.2.3	Perform internal and external scans after any significant change[6].
PCI-DSS Req.	***Requirement 12*** ***Maintain a policy that addresses information security for all personnel***
12.1	Stanford & Green's-DSS Security Policy PCI shall accomplish the following:
12.1.1	Addresses all applicable PCI DSS requirements.
12.1.3	Include a review at least annually and updates when the environment changes.
12.2	Daily operational security procedures must comply with the Operational Security Standard.
12.3	Usage policies for critical technologies, which define proper use of these technologies, have been developed which:
12.3.1	Require explicit approval by authorised parties.
12.3.2	Stipulate authentication requirements for use of the technology.
12.3.3	List of all such devices and personnel with access.
12.3.5	Define acceptable uses of the technology.
12.3.6	Define acceptable network locations for the technologies.
12.3.8	Automatic disconnect sessions for remote-access technologies after a specific period of inactivity.
12.4	Information security responsibilities for all personnel are clearly defined within the security policy and procedures.
12.5	The following information security management responsibilities are to be assigned to an individual or team:
12.5.3	Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
12.6	A formal security awareness program which is designed to make all personnel aware of the importance of cardholder data security has been implemented.
12.6.1	Personnel are required to undertake security awareness training upon hire and at least annually.
12.6.2	That there is an established process for engaging service providers including proper due diligence prior to engagement.

12.8	Policies and procedures to manage service providers must be implemented and maintained. These are to include:
12.8.1	A maintained list of service providers.
12.8.2	A written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.
12.8.3	There is an established process for engaging service providers including proper due diligence prior to engagement.
12.8.4	That there is a program to monitor service provider annually.

Appendix 2 - Glossary

CDE	Cardholder Data Environment - The people, processes and technology that store, process or transmit cardholder data or sensitive authentication data, including any connected system components.
PA-DSS	PCI DSS Payment Application Data Security Standard.
PCI	Acronym for Payment Card Industry.
PCI-DSS	Payment Card Industry Data Security Standard.
PCI SSC	Payment Card Industry Security Standards Council.
PED	PIN entry device.
POI	Acronym for “Point of Interaction,” the i electronic transaction-acceptance product, a POI consists of hardware and software and is hosted in acceptance equipment to enable a cardholder to perform a card transaction. The POI may be attended or unattended. POI transactions are typically integrated circuit (chip) and/or magnetic-stripe card-based payment transactions.
PTS	Payment Card Industry PIN Transaction Security, PTS is a set of modular evaluation requirements managed by PCI Security Standards Council, for PIN acceptance POI terminals. Please refer to www.pcisecuritystandards.org.
VT	A virtual terminal is web-browser-based access to an acquirer, processor or third party service provider website to authorise payment card transactions, where the merchant manually enters payment card data via a securely connected web browser. Unlike physical terminals, virtual terminals do not read data directly from a payment card. Because payment card transactions are entered manually, virtual terminals are typically used instead of physical terminals in merchant environments with low transaction volumes.