

THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI-DSS)

NON-TECHNICAL CONSIDERATIONS FOR CHARITIES

WHAT IS THE PCI-DSS?

- It is a worldwide data security standard governing the secure handling of cardholder data.
- It comprises a series of technical and operational requirements. The current requirements (as at September 2011) are summarised as 6 key control objectives which translate into 12 key requirements.

Control Objectives		Requirements	
1	Build and maintain a secure network	1	Install and maintain a firewall configuration to protect cardholder data
		2	Do not use vendor supplied defaults for system passwords and other security parameters
2	Protect cardholder data	3	Protect stored cardholder data
		4	Encrypt transmission of cardholder data across open, public networks
3	Maintain a vulnerability management program	5	Use and regularly update anti-virus software or programs
		6	Develop and maintain secure systems and applications
4	Implement strong access control measures	7	Restrict access to cardholder data by business need-to-know
		8	Assign a unique ID to each person with computer access
		9	Restrict physical access to cardholder data

5	Regularly monitor and test networks	10	Track and monitor all access to network resources and cardholder data
		11	Regularly test security systems and processes
6	Maintain an Information Security Policy	12	Maintain a policy that addresses information security for all personnel

- Its purpose is to ensure that businesses storing, processing and transmitting cardholder data have optimum security measures in place to reduce vulnerabilities and prevent fraud, in order to provide a greater level of protection for consumers.
- The first PCI-DSS was released in December 2004 (Version 1.0) and has been subsequently modified through three updated releases:
 - Version 1.1 released September 2006
 - Version 1.2 released October 2008
 - Version 2.0 released October 2010
- The standard was developed by, and is maintained by, the Payment Card Industry Security Standards Council – a collective formed from the five major card brands AmEx, Discover, JCB, MasterCard & Visa.
- The Council continually monitor and evaluate market trends and emerging security threats and use this intelligence, along with input from participating organisations, to determine the content and timing of releases of the standard. It is expected that future updates will be released every 18-24 months.
- Full copies of the PCI-DSS and all relevant supporting documentation can be downloaded from the PCI Security Standards Council website: <https://www.pcisecuritystandards.org/>

HOW DOES COMPLIANCE WORK?

- Compliance with the PCI-DSS is mandatory for any entity that accepts payments under the five member card brands and also for entities that provide services where the provision of the services results in storing, processing and transmitting cardholder data to merchants and/or other service providers.
- Compliance for all such entities is irrespective of the scope/nature of the business activities.

- Charities and non-profit organisations that accept card payments under any of the five member card brands will meet the definition of a “merchant” for the purposes of PCI-DSS and will therefore need to be compliant, irrespective of the annual card transaction volumes.
- Compliance is enforced by the founding members of the Council (AmEx, Discover, JCB, MasterCard & Visa).
- PCI have powers to suspend card services, enforce audits and levy fines for non-compliance.
- Merchants/service providers are generally categorised based on their annual volume of card transactions.
- Compliance requirements for top-tier (high volume) merchants/service providers are usually:
 - Annual audit by a PCI Qualified Security Assessor (PCI-QSA)
 - Report on Compliance/Attestation of Compliance
 - Quarterly network scans by a PCI Approved Scanning Vendor (PCI-ASV), clean passing scan required
- Compliance requirements for lower-tier (lower volume) merchants/service providers are usually:
 - Annual self-assessment using the PCI Self Assessment Questionnaire (PCI-SAQ)
 - Attestation of compliance
 - Quarterly network scans by a PCI Approved Scanning Vendor (PCI-ASV), clean passing scan required
 - In some cases the SAQ may also need to be validated by a PCI Qualified Security Assessor (PCI-QSA)
- Guidance on merchant definitions/volumes and compliance requirements is available on the main card brand websites:

American Express:

https://www260.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=merchinfo&ln=en&frm=GB&tabbed=merchantLevel

MasterCard:

http://www.mastercard.com/us/company/en/whatwedo/determine_merchant.html

Visa:

http://www.visaeurope.com/en/businesses_retailers/payment_security/merchants.aspx

- For specific advice on which compliance requirements are applicable for your activities and volumes you will need to check with your own acquirer/bank and with your card payment brands. Full guidance and support can also be provided by PCI Qualified Security Assessors (PCI-QSAs) and PCI Approved Scanning Vendors (PCI-ASVs)

WHAT ARE THE KEY CONSIDERATIONS FOR CHARITIES?

At first glance the 12 requirements within the PCI-DSS may appear to be largely technical and can therefore result in a misperception that compliance is only concerned with operating secure IT infrastructures and networks, and is therefore the responsibility of the IT team.

However, whilst the IT aspects of the requirements are significant and should not be underestimated, the PCI-DSS also has a much wider scope in promoting the adoption of business-wide comprehensive security strategies and policies.

A further consideration is that the standard covers all forms of cardholder data. In addition to data recorded, held and transmitted electronically within systems applications, it also covers any cardholder data being recorded, handled and stored on hard copy, being stored within digital images, being stored within voice recordings, and so on, and the compliance requirements therefore often extend to business areas and processes beyond the remit of the IT team.

Compliance requirements must therefore be approached from a global business perspective, and compliance assessments need to cover multiple business functions to encompass all relevant business systems and processes and all relevant technical and physical operations.

A key element of any compliance assessment is therefore to identify all business activities where there is a touch-point with cardholder data – whether this is receiving/recording card data, handling/processing card data, storing card data or transmitting/transferring card data. And for each of these touch-points to then review all relevant business systems, processes and security measures.

For charities, in addition to the IT infrastructure/network and the application development processes, some or all of the following non-technical business and operational areas may also therefore need to be reviewed for PCI-DSS compliance considerations:

Corporate Strategy & Policy

- Is there a corporate Information Security Policy in place?

- Is the policy reviewed annually?
- Is the policy published?
- Is there a formal security awareness programme in place?
- Are staff educated at induction and at least annually thereafter?
- Are all staff aware of the policy and their security responsibilities?
- Do staff formally acknowledge their awareness/responsibilities?

Premises & Facilities

- Is there a formal visitor policy in place?
- Are visitors issued a physical token to be surrendered on departure?
- Are visitor logs retained for 3 months?
- Are visitors always accompanied by staff?
- Are visitors easily visually distinguishable from staff?
- Is there a "stop & challenge" policy in place?
- Are there restricted access areas?
- What rules determine access to restricted areas?
- What overall premises security measures are in place?
- How is incoming mail handled/processed/protected?

Direct Marketing/Supporter Services

- Are card payments solicited through direct marketing activities such as direct mail, inserts, door drops, OTP advertising, in/outbound telemarketing?
- Are card payments solicited through events and community fundraising activities?
- Are postal card payments received in-house?
- Are telephone card payments received in-house?
- What in-house processes are used for recording card data?
- What in-house processes are used transferring card data between internal people, departments and systems?
- Is card data received in-house forwarded to external recipients such as 3rd party outsource suppliers?
- Are there audit trails for the handling and processing of card payments?
- Are hard copy records of card data retained?
- Are forms containing card data scanned and retained as digital images?
- Is card data added to database systems and applications?
- What security measures are in place for protecting hard copy records, digital images and voice recordings?
- How is access to hard copy records, digital images and database systems controlled?
- Are response handling and fulfilment activities outsourced?
- Do outsource suppliers forward card data to in-house recipients?

- Are there regular givers giving via continuous credit?
- How are the continuous credit collections administered?
- Do staff have look-up facilities for in-house systems which allow card data to be viewed?
- Do staff have web enabled look-up facilities into outsource suppliers' systems which allow card data to be viewed?

Online Marketing

- Are one-off card donations/continuous credit giving solicited via the website?
- What type of online payment applications are used – real-time payment gateways, hosted pages, off-line?
- Are the payment pages/payment applications secure and PCI-compliant?
- Is card data transferred from the online application to in-house recipients or to other 3rd party outsource suppliers?
- Is card data collected online added to in-house database systems and applications?
- What transfer formats and methods are used?

Finance

- Are physical/virtual terminals used to process card payments?
- What printed receipts are produced?
- Are printed records/reports containing card data produced and retained?
- How is access to printed records/reports controlled?
- Are there audit trails for the handling and processing of card payments?
- How are chargebacks and refunds handled?

Physical Archive/Records Control

- Are hard copy records of card data retained?
- Is there a documented archive and retention policy?
- Is there a dedicated in-house archive facility?
- What security measures are in place to protect the archive facility?
- How is access to the archive area controlled?
- Is there a policy regarding the removal of items from the archive?
- Are hard copy records sent off-site for storage?
- Are secure off-site storage facilities used?
- Are 3rd party/shared storage facilities used?
- Are hard copy records disposed of using secure destruction methods at the end of the retention period?

Procurement

- Are any card functions outsourced to 3rd party suppliers?
- How is supplier compliance managed and monitored?
- Is compliance a contractual requirement?

Regional Offices

- Are there regional/branch offices?
- Are postal card payments received at regional offices?
- Are telephone card payments received at regional offices?
- What processes are used for recording and processing card data?
- Is card data received at regional offices forwarded to Head Office and if so, what forwarding format and methods are used?
- Are there audit trails for the handling/processing/transfer of card data?
- Are hard copy records/copies of card data retained?
- What security measures and access controls are in place for protecting hard copy records?
- Are volunteers/temporary staff used for work involving card data?
- What overall premises security measures are in place?

Field Activities

- Are there any field/F2F/D2D activities which generate card payments?
- What systems are used to record and process card payments?
- Are payments processed with the cardholder present or are card details recorded for subsequent processing?
- Is card data recorded on hard copy?
- Is card data forwarded to a Regional Office or Head Office?
- What format and methods are used for forwarding card data?
- Are there audit trails for the handling/processing/transfer of card data?
- Are field/F2F/D2D activities outsourced to 3rd party suppliers?
- Do outsource suppliers forward card data to in-house recipients?

SUMMARY

The extent of the impact of the PCI-DSS requirements on charities may vary greatly from charity to charity depending on:

- The nature/scope of the charity's business activities

- How the charity is structured for business delivery
- What systems, processes, routines and workflows are used for business delivery

It is therefore recommended that the on-going compliance process be managed by a cross-functional team to ensure that all relevant business areas and all relevant business systems and processes are included for assessment.

SUPPORT & RESOURCES

General support information is available from the PCI Security Standards Council website:

<https://www.pcisecuritystandards.org/>

The website includes:

- PCI documentation – standards, SAQs, attestations of compliance, etc
- PCI support material - fact sheets, user guidelines, FAQs, etc
- News updates
- Listings of PCI Qualified Security Assessors (PCI-QSAs)
- Listings of PCI Approved Scanning Vendors (PCI-ASVs)

More specific support and guidance can be obtained from:

- Your acquirer
- Your bank
- Your payment brands
- PCI-QSAs
- PCI-ASVs

Information compiled by: Sue Maccabe, Consultant Business Analyst
September 2011

For more information visit www.docdataresponse.co.uk t.01993 770600 e. info@docdataresponse.co.uk
OR Sue Maccabe e. sue.maccabe@dotjoining.co.uk