The Design Society

Information Security Policy

Policies and Forms That Conform to PCI DSS SAQ A

Version 2.0

June 2014

About this Document

This document contains The Design Society information security policies. This document is for internal use only and is not to be distributed.

The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, The Design Society's cardholder environment consists only of payments taken through the website processed entirely by WorldPay or PayPal. The environment does not include storage of cardholder data on any computer system. If this were to ever change it is the responsibility of The Design Society to determine the appropriate compliance criteria and implement additional policies and controls as needed.

Revision History

Version	Date	Author	Description of Change
1	27/04/2014	Rebecca Axford	Security Policy Created
2	16/03/2016	Rebecca Axford	Review of Policy, update to Security Policy Custodians.

Table of Contents

Introduction

To safeguard The Design Society's information technology resources and to protect the confidentiality of data, adequate security measures must be taken. This Information Security Policy reflects The Design Society's commitment to comply with required standards governing the security of sensitive and confidential information.

The Design Society can minimize inappropriate exposures of confidential and/or sensitive information, loss of data and inappropriate use of computer networks and systems by complying with reasonable standards (such as Payment Card Industry Data Security Standard), attending to the proper design and control of information systems, and applying sanctions when violations of this security policy occur.

Security is the responsibility of everyone who has access to The Design Society's confidential information including cardholder data. It is the responsibility of employees, contractors, business partners, and agents of The Design Society to comply with this policy

and to protect The Design Society's confidential information (including cardholder data). Each should become familiar with this policy's provisions and the importance of adhering to it when using computers, networks, data and other information resources that contain or have access to The Design Society's confidential information. Each is responsible for reporting any suspected breaches of its terms.

Purpose/Scope

The primary purpose of this security policy is to establish rules to insure the protection of confidential and/or sensitive information stored or transmitted electronically and to ensure protection of The Design Society's information technology resources. The policy assigns responsibility and provides guidelines to protect The Design Society's systems and data against misuse and/or loss.

This security policy applies to all Administrators and Members of The Design Society who have access to any confidential information online or in paper form.

This security policy applies to all aspects of information technology resource security including, but not limited to, accidental or unauthorized destruction, disclosure or modification of hardware, software, networks and/or data.

This security policy has been written to specifically address the security of data used by the Payment Card Industry. Credit card data stored, processed or transmitted by The Design Society must be protected and security controls must conform to the Payment Card Industry Data Security Standard (PCI DSS). Sensitive credit card data is defined as the Primary Account Number (PAN), Card Validation Code (CVC, CVV2, CVC2), and any form of magnetic stripe data from the card (Track 1, Track 2).

Security Policy Ownership and Responsibilities

It is the responsibility of the custodians of this security policy to publish and disseminate these policies to all relevant Design Society system users (including vendors, contractors, and business partners). Also, the custodians must see that the security policy addresses and complies with all standards The Design Society is required to follow (such as the PCI DSS). This policy document will also be reviewed at least annually by the custodians (and any relevant data owners) and updated as needed to reflect changes to business objectives or the risk environment.

Questions or comments about this policy should be directed to the custodians of this policy as detailed in the table below:

Table 1 -- Security Policy Custodians

Name	Title	Phone	E-mail Address
Rebecca Axford	Administrator		contact@designsociety.org
Antonio Magdić	Website Developer		webmaster@designsociety.org
Tim McAloone	Treasurer		tmca@dtu.dk

Restrict Access to Sensitive Data and System Components

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

1.0 Restrict Physical Access to Cardholder Data

1.1 Securing Hard Copy Materials

- The Design Society does not hold hard copy materials containing cardholder data but will nevertheless define procedures required for protecting paper and hard copy materials (which includes paper receipts, mail, reports, and faxes) containing cardholder data within all facility locations in case the procedure should become necessary. See appendix B (PCI-DSS Requirement 9.6)

1.2 Secure Media Containing Sensitive Data

- The Design Society will define specific procedures required for controlling the internal or external distribution of any kind of media containing cardholder data in the event that such distribution takes place. The Design Society will always maintain strict control over the storage and accessibility of both hardcopy and electronic media that contains cardholder data. (PCI-DSS Requirement 9.7, 9.9)
- All forms of media containing cardholder data is required to be classified as sensitive and must be labeled so as to be identified as confidential data. (PCI-DSS Requirement 9.7.1)
- All media containing sensitive cardholder data sent outside the facility must be transferred by secured courier or other delivery method that can be accurately tracked. Log all transfers of media containing cardholder data. Logs must show management approval, and tracking information. Retain media transfer logs. (PCI-DSS Requirement 9.7.2)
- Management approval (The President) is required prior to moving any and all media containing cardholder information out of a secured area (especially when media is distributed to individuals). (PCI-DSS Requirement 9.8)
- Periodic inventory of stored media containing cardholder data must be performed and documentation must be retained showing these inventories were performed. (PCI-DSS Requirement 9.9)

1.3 Media Destruction Policies

- Media containing cardholder data must be destroyed when it is no longer needed for business or legal reasons. (PCI-DSS Requirement 9.10)
- The Design Society defines that shredding will be used to destroy any hard copy materials containing cardholder data beyond reconstruction. When cardholder data is destroyed by shredding this will be recorded in a log. (PCI-DSS Requirement 9.10.1)

Maintain an Information Security Policy

Without strong security policies and procedures many layers of security controls become ineffective at preventing data breach. Unless consistent policy and practices are adopted and followed at all times, security controls break down due to inattention and poor maintenance. The following documentation policies address maintaining The Design Society security policies described above.

2.0 Maintain a Security Policy for Employees and Contractors

A strong security policy sets the security tone for The Design Society 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.

2.1 Policies For Sharing Data With Service Providers

If cardholder data is shared with service providers (such as, back-up tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes), the following policies and procedures must be followed:

- The Design Society must maintain a documented list of any service provider that is given cardholder data, provided direct access to the cardholder network, or can affect the security of the cardholder network. (PCI-DSS Requirement 12.8.1)
- Any written agreement with a service provider that is given cardholder data, provided direct access to the cardholder network, or can affect the security of the cardholder network, must include an acknowledgement of the service providers responsibility for securing all cardholder data they receive from The Design Society (PCI-DSS Requirement 12.8.2)
- Prior to engaging with a service provider that is given cardholder data, provided direct access to the cardholder network, or can affect the security of the cardholder network, The Design Society will conduct due diligence and follow an established process to ensure that the security of cardholder data within the service provider's network has been addressed. (PCI-DSS Requirement 12.8.3)
- No Service Providers are given cardholder data or access to the cardholder network. If this were to ever happen then The Design Society will have an ongoing program to monitor the PCI DSS compliance status of any service provider that is given cardholder data, provided direct access to the cardholder network, or can affect the security of the cardholder network. (PCI-DSS Requirement 12.8.4)

Appendix A – Agreement To Comply

Agreement to Comply with Information Security Policies

All Administrators, members or contractors working with sensitive cardholder data must submit a signed paper copy of this form. The Design Society management will not accept modifications to the terms and conditions of this agreement.

_____
Administrator/Member/Contractor's Printed Name

_____
Administrator/Member/Contractor's Department

_____
Administrator/Member/Contractor's Telephone Number

_____
Administrator/Member/Contractor's Physical Address and Mail Location

I, the user, agree to take all reasonable precautions to assure that The Design Society internal information, or information that has been entrusted to The Design Society by third parties such as members, will not be disclosed to unauthorized persons. At the end of my employment or contract with The Design Society I agree to return to The Design Society all information to which I have had access as a result of my position with The Design Society. I understand that I am not authorized to use this information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal Design Society manager who is the designated information owner.

I agree to abide by the security policy. I understand that non-compliance may be cause for disciplinary action up to and including system privilege revocation, dismissal from The Design Society, and perhaps criminal and/or civil penalties.

I agree to choose a difficult-to-guess password for any device which has access to The Design Society's confidential information, I agree not to share this password with any other person, and I agree not to write this password down unless it has been transformed in an unrecognizable way.

I also agree to promptly report all violations or suspected violations of information security policies to the Treasurer and President of The Design Society.

_____
Employee/Contractor's Signature

Appendix B – Design Society Procedure for Securing Hard Copy Materials

At the moment The Design Society does not have any access to hard copy materials containing sensitive cardholder data. If the Design Society were ever to access hard copy materials containing sensitive cardholder data the following procedures will be adhered to:

*All media must be physically secured in a locked filing cabinet, cupboard or safe. (PCI requirement 9.6)

*All media must be clearly labelled as confidential. (PCI requirement 9.7.1)

*If any hard copy media were ever to be sent it must be sent by a secure carrier or other delivery method that can be accurately tracked (PCI requirement 9.7.2)

*All media containing cardholder data must be destroyed by shredding when it is no longer needed for business or legal reasons. It must be shredded so that it cannot be reconstructed. (PCI requirement 9.10, 9.10.1)