# Campbell Harris Tutors Ltd

# Credit Card Security Policies

### 28th JUNE 2017

**CONFIDENTIAL INFORMATION**

*Note: This is a policy template and may need modification to fit your specific business environment. This document is intended as an aid to assist you in developing policies and procedures for your business and systems that adhere to the Payment Card Industry Data Security Standard. Adopting these policies does not guarantee that you will become PCI complaint or that your systems are secure. Trustwave makes no representations or warranties and specially disclaims any and all representation and warranties regarding these policies.*

# Introduction and Scope

### Introduction

This document explains Campbell Harris Tutors Ltd's credit card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. Campbell Harris Tutors Ltd management is committed to these security policies to protect information utilized by Campbell Harris Tutors Ltd in attaining its business goals. All employees are required to adhere to the policies described within this document.

### Scope of Compliance

The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, Campbell Harris Tutors Ltd's cardholder dataflow includes only paper media. Electronic storage of cardholder data is not conducted or permitted. Due to the limited nature of the in-scope environment, this document is intended to meet the PCI requirements as defined in Self-Assessment Questionnaire (SAQ) B ver. 1.2, October, 2008. Should Campbell Harris Tutors Ltd implement additional acceptance channels, begin storing, processing, or transmitting cardholder data in electronic format, or otherwise become ineligible to validate compliance under SAQ B it will be the responsibility of Campbell Harris Tutors Ltd to determine the appropriate compliance criteria and implement additional policies and controls as needed.

# Requirement 3: Protect Stored Cardholder Data

### Prohibited Data

Sensitive authorization data will be retained only until completion of the authorization of a transaction. Storage of sensitive authorization data post-authorization is forbidden. Specifically, sensitive authorization data includes the following:

- ❑ The full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. (PCI requirement 3.2.1)

- ❑ The card verification code or value (three- or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions. (PCI requirement 3.2.2)

- ❑ The personal identification number (PIN) or the encrypted PIN block. (PCI requirement 3.2.3)

### Displaying PAN

Campbell Harris Tutors Ltd will mask the display of PANs (primary account numbers), and limit viewing of PANs to only those employees and other parties with a legitimate need. A properly masked number will show only the first six and the last four digits of the PAN. (PCI requirement 3.3)

# Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

### Transmission of Cardholder Data

Sending unencrypted PANs by end-user messaging technologies is prohibited. Examples of end-user technologies include email, instant messaging and chat. (PCI requirement 4.2)

# Requirement 7: Restrict Access to Cardholder Data by Business Need to Know

**Limit Access to Cardholder Data**

Access to Campbell Harris Tutors Ltd's cardholder data is limited to only those individuals whose job requires such access. (PCI requirement 7.1)

Access limitations must include the following:

Restriction of access rights to cardholder data to the least access needed to perform job responsibilities.

Access to cardholder data is based on an individual's job classification and function.

Access to cardholder data will be granted only after completing an authorization request form. This form must be signed by management.

# Requirement 9: Restrict Physical Access to Cardholder Data

## Physically Secure all Paper Containing Cardholder Data

Hard copy materials containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:

- ❑ Printed reports containing cardholder data are to be physically retained, stored or archived only within secure Campbell Harris Tutors Ltd office environments, and only for the minimum time deemed necessary for their use. (PCI requirement 9.6)

- ❑ All hardcopy media containing cardholder data must be stored in a secure and locked container (e.g. locker, cabinet, desk, storage bin). (PCI requirement 9.6)

- ❑ Hardcopy material containing cardholder data should never be stored in unlocked or insecure containers or open workspaces. (PCI requirement 9.6)

- ❑ All hardcopy material containing cardholder data must be easily distinguishable through labeling or other methods. (PCI requirement 9.7.1)

- ❑ All confidential or sensitive hardcopy material must be sent or delivered by a secured courier or other delivery methods that can be accurately tracked. (PCI requirement 9.7.2)

- ❑ At no time is printed material containing cardholder data to be removed from any Campbell Harris Tutors Ltd data center or computer room without prior authorization from management. (PCI requirement 9.8)

- ❑ Custodians of hardcopy media containing cardholder data must perform an inventory of the media at least annually. Results of inventories shall be recorded in an inventory log. (PCI requirement 9.9)

## Destruction of Data

All media containing cardholder data must be destroyed when no longer needed for business or legal reasons. (PCI requirement 9.10)

Hardcopy media must be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed. (PCI requirement 9.10.1)

# Requirement 12: Maintain a Policy that Addresses Information Security for Employees and Contractors

## Security Policy

Campbell Harris Tutors Ltd shall maintain a security policy that addresses how the company will protect cardholder data. This policy must be reviewed at least annually, and must be updated as needed to reflect changes to business objectives or the risk environment. (PCI requirement 12.1.1, 12.1.3)

Employees shall not use or otherwise employ employee-facing technologies to store, process or otherwise handle cardholder data. Employee-facing technologies include remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), email, and internet usage. (PCI requirement 12.3)

The policies and procedures delineated in this document will apply to all employees and contractors involved in the processing, storage, or other handling of cardholder data. (PCI requirement 12.4)

### Incident Response Policy

The Principal shall establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. (PCI requirement 12.5.3)

### Incident Identification

Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents that an employee might recognize in their day to day activities include, but are not limited to,

- ❑ Theft, damage, or unauthorized access (e.g., papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry)
- ❑ Fraud – Inaccurate information within databases, logs, files or paper records

### Reporting an Incident

A Principal should be notified immediately of any suspected or real security incidents involving cardholder data:

- ➢ Contact a Principal to report any suspected or actual incidents. The Internal Audit's phone number should be well known to all employees and should page someone during no-business hours.

- ➢ No one should communicate with anyone outside of their supervisor(s) or the Principal about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by a Principal

- ➢ Document any information you know while waiting for the Principal to respond to the incident. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.

### Incident Response

Responses can include or proceed through the following stages: identification, severity classification, containment, eradication, recovery and root cause analysis resulting in improvement of security controls.

Contain, Eradicate, Recover and perform Root Cause Analysis

1. Notify applicable card associations.

#### Visa

Provide the compromised Visa accounts to Visa Fraud Control Group within ten (10) business days. Account numbers must be securely sent to Visa as instructed by the Visa Fraud Control Group. It is critical that all potentially compromised accounts are provided. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information. See Visa's "What to do if compromised" documentation for additional activities that must be performed. That documentation can be found at http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_what_to_do_if_compromised.pdf

**MasterCard**

Contact your merchant bank for specific details on what to do following a compromise. Details on the merchant bank (aka. the acquirer) can be found in the Merchant Manual at http://www.mastercard.com/us/wce/PDF/12999_MERC-Entire_Manual.pdf.

**Discover Card**

Contact your relationship manager or call the support line for further guidance.

2. Alert all necessary parties. Be sure to notify:

    a. Merchant bank

    b. Police

    c. Local authorities

3. Collect and protect information associated with the intrusion. In the event that forensic investigation is required the Principal will work with legal and management to identify appropriate forensic specialists.

4. Eliminate the intruder's means of access and any related vulnerabilities.

5. Research potential risks related to or damage caused by intrusion method used.

## Root Cause Analysis and Lessons Learned

Not more than one week following the incident, the Principals and all affected parties will meet to review the results of any investigation to determine the root cause of the compromise and evaluate the effectiveness of the *Incident Response Plan*. Review other security controls to determine their appropriateness for the current risks. Any identified areas in which the plan, policy or security control can be made more effective or efficient, must be updated accordingly.

## Security Awareness

Campbell Harris Tutors Ltd shall implement and maintain an security awareness program with the intent of ensuring all employees that process, store, or are otherwise involved in handling cardholder data are aware of the importance of cardholder data security. (PCI requirement 12.6)

Campbell Harris Tutors Ltd will ensure employees receive security awareness training upon hire and at least annually. The security awareness program must provide multiple methods of educating employees, including posters, letters, memos, web-based training, meetings, or promotions. (PCI requirement 12.6.1)

## Service Providers

Campbell Harris Tutors Ltd will implement policies and procedures to manage service providers. (PCI requirement 12.8) This process must include the following:

❑ Maintain a list of service providers (PCI requirement 12.8.1)

❑ Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of the cardholder data the service providers possess (PCI requirement 12.8.2)

❑ Implement a process to perform proper due diligence prior to engaging a service provider (PCI requirement 12.8.3)

❑ Monitor service providers' PCI DSS compliance status (PCI requirement 12.8.4)

Reviewed May 2023

**CONFIDENTIAL INFORMATION**