CREDIT CARD PROCESSING AND SECURITY POLICY

Note:-

The purpose of this policy is to define the guidelines for accepting and processing credit cards and storing personal cardholder information. The policy will help to ensure that cardholder information supplied to G&L Consultancy Ltd is secure and protected. The company is complying with credit card company requirements and the Payment Card Industry Data Security Standard.

This Policy Document is approved for use:

See Page 9 of 9

ISSUE	REV	DATE	DETAILS OF REVISION	AUTHORISED BY
01	00	01.09.15	Issue of new format	J. Lewis
01	01	01.09.16	Reviewed – No Change	M. Skinner
01	02	23.01.17	Reviewed – No Change	M. Skinner
01	03	22.01.18	Reviewed – No Change	M. Skinner
01	04	20.01.19	Reviewed – No Change	M. Skinner
01	05	22.01.20	Reviewed – No Change	M. Skinner
01	06	04.01.21	Reviewed – No Change	M. Skinner
01	07	12.01.22	Reviewed – No Change	M. Skinner
01	08	05.01.23	Reviewed – No Change	M. Skinner
01	09	12.01.24	Reviewed – No Change	M. Skinner

Confidential information

Purpose

The purpose of this policy is to define the guidelines for accepting and processing credit cards and storing personal cardholder information. The policy will help to ensure that cardholder information supplied to G&L Consultancy Ltd is secure and protected. The company is complying with credit card company requirements and the Payment Card Industry Data Security Standard.

Definitions

- Payment Card Industry (PCI) Data Security Standard:

  THE PCI DSS is designed to ensure that all merchants that store, process, or transmit Visa cardholder data, protect it properly. To achieve compliance, merchants and service providers must adhere to the Payment Card Industry (PCI) Data Security Standard.

- PCI:

  The PCI Standard is the result of collaboration between the four major credit card brands to develop a single approach to safeguarding sensitive data. The PCI standard defines a series of best practices for handling, transmitting and storing sensitive data.

- Cardholder Data:

  Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, social security number, Card Validation Code CVC 2 (MasterCard), Card Verification Value CVV2 (VISA), Cardmember ID (Discover) or CID - Card Identification Number (American Express) (e.g., three- or four-digit value printed on the front or back of a payment card.

- System Administrator / Data Custodian:

  An individual who performs network / system administration duties and/or technical support of network / systems that are accessed by other people, systems, or services. Only full-time employees of the Company and / or third party vendors approved by the Company may function as system / network administrators and / or data custodians.

Introduction and Scope

Introduction

This document explains G&L Consultancy Ltd's credit card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. G&L Consultancy Ltd's management is committed to these security policies to protect the information used by G&L Consultancy 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, G&L Consultancy Ltd's cardholder environment consists only of payment in person or over the telephone via 'SagePay'. The environment does not include storage of cardholder data on any computer system.

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. 3.0, released February 2014.

Should G&L Consultancy 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 G&L Consultancy Ltd to determine the appropriate compliance criteria and implement additional policies and controls as needed.

Requirement 3: Protect Stored Cardholder Data

Prohibited Data

G&L Consultancy Ltd does not retain sensitive authentication data post-authorisation. Employees are instructed not to record such information. If any information is written down this is immediately shredded so that it is unrecoverable. (PCI Requirement 3.2)

Payment systems must adhere to the following requirements regarding the non-storage of sensitive authentication data after authorisation (even if encrypted):

- The full contents of any track data from the magnetic stripe (located on the back of a card, equivalent data contained on a chip or elsewhere) are not stored under any circumstance. (PCI Requirement 3.2.1)
- The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored under any circumstance. (PCI Requirement 3.2.2)
- The personal identification number (PIN) or the encrypted PIN block are not stored under any circumstance. (PCI Requirement 3.2.3)

Displaying PAN

G&L Consultancy 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 no more than 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 G&L Consultancy Ltd's cardholder system components and data is limited to only those individuals whose jobs require such access. (PCI Requirement 7.1)

Access limitations include the following:

- Access rights for privileged user IDs must be restricted to the least privileges necessary to perform job responsibilities. (PCI Requirement 7.1.2)
- Privileges must be assigned to individuals based on job classification and function (also called "role-based access control"). (PCI Requirement 7.1.3)

Requirement 9: Restrict Physical Access to Cardholder Data

Physically Secure all Media 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:

- All media must be physically secured. (PCI requirement 9.5)
- Strict control must be maintained over the internal or external distribution of any kind of media containing cardholder data. These controls shall include: (PCI Requirement 9.6)
    - Media must be classified so the sensitivity of the data can be determined. (PCI Requirement 9.6.1)

- Media must be sent by a secure carrier or other delivery method that can be accurately tracked. (PCI Requirement 9.6.2)

- Management approval must be obtained prior to moving the media from the secured area. (PCI Requirement 9.6.3)

- Strict control must be maintained over the storage and accessibility of media containing cardholder data. (PCI Requirement 9.7)

Destruction of Data

All media containing cardholder data must be destroyed when no longer needed for business or legal reasons. (PCI requirement 9.8)

Hard copy media must be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed. (PCI requirement 9.8.1.a)

Containers storing information waiting to be destroyed must be secured (locked) to prevent access to the contents by unauthorised personnel. (PCI requirement 9.8.1.b)

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

Security Policy

G&L Consultancy Ltd shall establish, publish, maintain and disseminate a security policy that addresses how the company will protect cardholder data. (PCI Requirement 12.1)

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)

Critical Technologies

G&L Consultancy Ltd shall establish usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data / digital assistants (PDAs), email and internet usage. (PCI requirement 12.3)

These policies must include the following:

- Explicit approval by authorised parties to use the technologies. (PCI Requirement 12.3.1)

- Acceptable uses of the technologies. (PCI Requirement 12.3.5)

Security Responsibilities

G&L Consultancy Ltd's policies and procedures will clearly define information security responsibilities for all personnel. (PCI Requirement 12.4)

Incident Response Policy

G&L Consultancy Ltd will 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 recognise in their day-to-day activities include, but are not limited to:

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

Reporting an Incident

The Accounts & Personnel Manager, Sally Monger, must be notified immediately of any actual or suspected security incidents involving cardholder data. If this is not possible, notify the Quality Director, Julie Lewis, instead.

Employees must not communicate details or generalities surrounding any actual or suspected incident to anyone outside the organisation. All communications with law enforcement agencies will be conducted by the Quality Director.

Team members must document / record any information they have about the incident. This should include the date, time and nature of the incident. Any information that can be provided will aid an appropriate response

Incident Response Policy (PCI requirement 12.10.1)

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

Contain, Eradicate, Recover and perform Root Cause Analysis

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. Refer to visa.com for more information.

MasterCard

- Contact your merchant bank for specific details on what to do following a compromise.

Discover Card

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

Alert all necessary parties. Be sure to notify:

- Merchant bank
- Police / Law Enforcement (if Visa payment data is compromised)

Perform an analysis of local legal requirements for reporting compromises everywhere clients were affected.

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

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

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

Root Cause Analysis and Lessons Learned

No more than one week following the incident, the Quality Director 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.

Other relevant security controls will also be reviewed 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

G&L Consultancy Ltd has produced this policy and will maintain the formal security awareness procedures detailed within it to ensure all personnel are aware of the importance of cardholder data security. (PCI Requirement 12.6)

Service Providers

G&L Consultancy Ltd has implemented and will maintain these policies and procedures to manage service providers. (PCI requirement 12.8)

- We maintain a list of service providers (PCI requirement 12.8.1)

  At present, our only service provider is SAGE PAY / Avalon

- The service providers are responsible for the security of the cardholder data the service providers possess (PCI requirement 12.8.2)

- Only reputable recognized service providers will be engaged, if in doubt due diligence must be carried out (PCI requirement 12.8.3)

- Service providers' PCI DSS compliance status will be monitored (PCI requirement 12.8.4)

- PCI DSS information about which requirements are managed by each service provider, and which are managed by the entity will be maintained. (PCI requirement 12.8.5)

CREDIT CARD PROCESSING AND SECURITY POLICY

The policy was reviewed and approved on 15th January 2024 following consultation with senior managers and workers.

Overall responsibility for the effectiveness of the policy lies with Julie Lewis, Quality Director. For more information, please contact this person: 01823 443 898

Director	Name	Signature	Date
Quality Director	Julie Lewis	Julie Lewis	15th Jan 2024
Technical Director	Paul Lewis	Paul Lewis	15th Jan 2024
Somerset Office	**Name**	**Signature**	**Date**
Health, Safety and Quality Manager	Mark Skinner	Mark Skinner	15th Jan 2024
Operations Manager	Darren Alway	Darren Alway	15th Jan 2024
Client Liaison Manager	James Ooyman	James Ooyman	15th Jan 2024
Finance and HR Manager	Sally Monger	Sally Monger	15th Jan 2024
Asbestos Removal & Air Test Manager	Jason Monger	Jason Monger	15th Jan 2024
Training Manager	Jack Leese	Jack Leese	15th Jan 2024
Survey Manager	Jo Haigh	Jo Haigh	15th Jan 2024
Northern Ireland Office	**Name**	**Signature**	**Date**
Northern Ireland Director	Alan Lewis	Alan Lewis	15th Jan 2024
Business Development & Personnel Manager	Karen Lewis	Karen Lewis	15th Jan 2024
Lab Manager	Colin Webb	Colin Webb	15th Jan 2024
Deputy NI Branch Manager	John McAleenan	John McAleenan	15th Jan 2024