

Connexion Developments Ltd

# Information Security Policy for SAQ B PCI DSS Compliance

Connexion Developments Ltd, Unit 3, Rainbow Court, Armstrog Way, Yate, Bristol, BS37 5NG

Tel: 01454 334 990 (0800 808 7799) E-mail: [sales@solenoid-valves.com](mailto:sales@solenoid-valves.com) [W:solenoid-valve.world](http://W:solenoid-valve.world)

## About this Document

This document contains the Connexion Developments Ltd information security policies. Detailed standards and processes that support this policy are described in associated standards and procedures documentation. This document is for internal use only and is not to be distributed.

Table 1 - Revision History

Version	Date	Author	Description of Change
1.0			Security Policy Created
1.2	November 2010		Security Policy Updates
2.0	April 2011	GWG	Update for PCI DSS v2.0
2.1	March 2012	TF	Update Doc references for NTP processes in Sect. 10
2.2	March 2012	ME	Formatting Updates
3.0	June 2014	JJB	Update for PCI DSS v3.0
3.1	July 2015	JDB	Update for PCI DSS v3.1 and format standardization
3.2	July 2016	MRS	Update for PCI DSS v3.2
4.0	July 2024	MAH	Update for PCI DSS v4.0

# Contents

<b>About this Document</b>	<b>1</b>
<b>Table 1 - Revision History</b>	<b>1</b>
Version	1
Date	1
Author	1
Description of Change	1
<b>Contents</b>	<b>2</b>
<b>Introduction</b>	<b>4</b>
<b>Purpose / Scope</b>	<b>4</b>
<b>Security Policy Ownership and Responsibilities</b>	<b>4</b>
<b>Additional Process and Standards Documents Referenced by this Security Policy</b>	<b>6</b>
<b>Table 2 – Security Process and Standards Documents Referenced by Policy</b> .....	<b>6</b>
<b>Protect Stored Cardholder Data</b>	<b>7</b>
3.1 Processes and mechanisms for protecting stored account data are defined and understood	
7	
3.3 Sensitive authentication data (SAD) is not stored after authorization	7
3.4 Access to displays of full PAN and ability to copy PAN is restricted	7
<b>Implement Strong Access Control Measures</b>	<b>7</b>
<b>7 Restrict Access to System Components and Cardholder Data by Business Need to Know</b>	
7	
7.2 Define and Assign Access to System Components and Data	8
<b>9 Restrict Physical Access to Cardholder Data</b> .....	<b>8</b>
9.4 Securely Store, Access, Distribute, and Destroy Media with Cardholder Data	8
9.5 Protect Point-of-Interaction (POI) Devices from Tampering and Unauthorized Substitution	
8	
<b>Maintain an Information Security Policy</b>	<b>9</b>
<b>12 Support Information Security with Organizational Policies and Programs</b> .....	<b>9</b>
12.1 Establish, Publish, Distribute, and Maintain the Information Security Policy	9
12.6 Security Awareness Program	10
12.8 Policies for Working with Third Party Service Providers (TPSPs)	10
12.10 Incident Response Plan Policies	10
<b>Appendix A – Management Roles and Responsibilities</b>	<b>12</b>
<b>Assignment of Management Roles and Responsibilities for Security</b> .....	<b>12</b>

**Appendix B - Agreement to Comply Agreement to Comply with Information Security Policies**

## Introduction

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

Connexion Developments Ltd can minimize inappropriate exposures of confidential 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 uses Connexion Developments Ltd's information technology resources. It is the responsibility of employees, contractors, business partners, and agents of Connexion Developments Ltd. Each should become familiar with this policy's provisions and the importance of adhering to it when using Connexion Developments Ltd's computers, networks, data and other information resources. Each is responsible for reporting any suspected breaches of its terms. As such, all information technology resource users are expected to adhere to all policies and procedures mandated by the Connexion Developments Ltd.

## Purpose / Scope

The primary purpose of this security policy is to establish rules to ensure the protection of confidential or sensitive information and to ensure protection of Connexion Developments Ltd's information technology resources. The policy assigns responsibility and provides guidelines to protect Connexion Developments Ltd's systems and data against misuse or loss.

This security policy applies to all users of computer systems, centrally managed computer systems, or computers that are authorized to connect to Connexion Developments Ltd's data network. It may apply to users of information services operated or administered by Connexion Developments Ltd (depending on access to sensitive data, etc.). Individuals working for institutions affiliated with Connexion Developments Ltd are subject to these same definitions and rules when they are using Connexion Developments Ltd's information technology resources.

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 or data.

This security policy has been written to specifically address the security of Credit Card Data used by Connexion Developments Ltd.

Credit card data stored, processed or transmitted with Connexion Developments Ltd's Merchant ID must be protected and security controls must conform to the Payment Card Industry Data Security Standard (PCI DSS).

Cardholder data within this document is defined as the full Primary Account Number (PAN) which may also appear in conjunction with Cardholder Name, Service Code, or Expiration date. Sensitive Authentication Data within this document is defined as the Card Validation Code (CVC, CVV2, CID, CAV2 and CVC2), Credit Card PIN, and any form of magnetic stripe data from the card (Track 1, Track 2). Account Data within this document is defined by any combination of Cardholder Data and Sensitive Authentication Data.

## Security Policy Ownership and Responsibilities

The Managing Director is the assigned custodian(s) of this Security Policy. It is the responsibility of the custodian(s) of this security policy to publish and disseminate these policies to all relevant Connexion Developments Ltd system users (including vendors, contractors, and business partners). In addition, the custodian(s) must see that the security policy addresses and complies with all standards Connexion Developments Ltd is required to follow (such as the PCI DSS). This policy document will also be reviewed at least annually by the custodian(s) (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 custodian(s) listed above.

# Additional Process and Standards Documents Referenced by this Security Policy

This policy document defines the Connexion Developments Ltd security policies relating to the protection of sensitive data and particularly credit card data. Details on Connexion Developments Ltd standards and procedures in place to allow these policies to be followed are contained in other documents referenced by this policy. Table 2 lists other documents that accompany this security policy document, which help define Connexion Developments Ltd data security best practices.

Table 2 – Security Process and Standards Documents Referenced by Policy

Document Name	Location or Custodian
System Hardening and Configuration Standards	Michael Freye
Full Data Retention and Storage Procedures	Michael Freye
Physical Security Procedures	Refresh It
Operating Procedures	Michael Freye
Security Awareness Training Process	Michael Freye
Service Provider Compliance Validation Process	Michael Freye
Incident Response Plan	Michael Freye

## Protect Stored Cardholder Data (No data stored)

3.1 Processes and mechanisms for protecting stored account data are defined and understood

Connexion Developments Ltd ensures documented processes and mechanisms for applying secure configurations to all system components are defined and understood, as follows:

- All security policies and operational procedures that are identified in this section shall be documented, kept up to date, in use, and known to all affected parties. (PCI DSS Requirement 3.1.1)
- Roles and responsibilities for performing activities in this section shall be documented, assigned, and understood.<sup>1</sup>

3.3 Sensitive authentication data (SAD) is not stored after authorization

Connexion Developments Ltd protects against the unauthorized disclosure of SAD by enforcing the following restrictions:

- SAD shall not be retained after authorization, even if encrypted. All sensitive authentication data received must be rendered unrecoverable upon completion of the authorization process. (PCI DSS Requirement 3.3.1)
- The full contents of any track shall not be retained upon completion of the authorization process. (PCI DSS Requirement 3.3.1.1)
- The card verification code shall not be retained upon completion of the authorization process. (PCI DSS Requirement 3.3.1.2)
- The personal identification number (PIN) and the PIN block shall not be retained upon completion of the authorization process. (PCI DSS Requirement 3.3.1.3)

3.4 Access to displays of full PAN and ability to copy PAN is restricted

In order to prevent the PAN being obtained by unauthorized individuals, Connexion Developments Ltd ensures that the full PAN is displayed only for those with a legitimate business need, as follows:

- PAN should be masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN. (PCI DSS Requirement 3.4.1)

## Implement Strong Access Control Measures

Access to system components and software within the cardholder data environment must be controlled and restricted to those with a business need for that access. This is achieved using active access control systems, strong controls on user and password management, and restricting physical access to critical or sensitive components and software to individuals with a “need to know”.

## 7 Restrict Access to System Components and Cardholder Data by Business Need to Know

Systems and processes must be in place to limit access to critical data and systems based on an individual’s need to know and according to job responsibilities.

---

<sup>1</sup> PCI Security Roles and Responsibilities Matrix



## 7.2 Define and Assign Access to System Components and Data

- Access is assigned to users, including privileged users, based on: (PCI DSS Requirement 7.2.2)
  - Job classification and function.
  - Least privileges necessary to perform job responsibilities.

## 9 Restrict Physical Access to Cardholder Data

Any physical access to data or systems that house cardholder data provide the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. Detailed physical security procedures should be developed and documented to meet the following policies.

### 9.4 Securely Store, Access, Distribute, and Destroy Media with Cardholder Data

- Connexion Developments Ltd will define specific procedures<sup>2</sup> to physically secure all media, including but not limited to computers, removable electronic media, paper receipts, paper reports and faxes. (PCI DSS Requirement 9.4.1)
- Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. (PCI DSS Requirement 9.4.1.1)
- Classify all media with cardholder data in accordance with the sensitivity of the data. (PCI DSS Requirement 9.4.2)
- Maintain strict control over the external distribution of media with cardholder data, including the following: (PCI DSS Requirement 9.4.3)
  - Media sent outside the facility is logged.
  - Send the media by secured courier or other delivery method that can be accurately tracked.
  - Logs must show management approval, and tracking information. Retain media transfer logs.
  - Ensure management approves all media with cardholder data that is moved from a secured area, including when media is distributed to individuals. (PCI DSS Requirement 9.4.4)
- Destroy hard-copy materials containing cardholder data when it is no longer needed for business or legal reasons, as follows: (PCI DSS Requirement 9.4.6)
  - Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.
  - Materials are stored in secure storage containers prior to destruction.

### 9.5 Protect Point-of-Interaction (POI) Devices from Tampering and Unauthorized Substitution

- Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. (PCI DSS Requirement 9.5.1)
- Maintain an up to date list of devices including the following: (PCI DSS Requirement 9.5.1.1)
  - Make and model of the device.
  - Location of the device.

---

<sup>2</sup> See the *Physical Security Procedures* document.

- Device serial number or other method of unique identification.
- Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been replaced with a fraudulent device). (PCI DSS Requirement 9.5.1.2)
  - The frequency of periodic POI device inspections and the type of inspections performed is defined in Connexion Developments Ltd's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. (PCI DSS Requirement 9.5.1.2)
- Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: (PCI DSS Requirement 9.5.1.3)
  - Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
  - Do not install, replace, or return devices without verification.
  - Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).
  - Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).

## Maintain an Information Security Policy

Without strong security policies and procedures, many of the 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 Connexion Developments Ltd security policies described in this document.

### 12 Support Information Security with Organizational Policies and Programs

A strong security policy sets the security tone for Connexion Developments Ltd 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.

#### 12.1 Establish, Publish, Distribute, and Maintain the Information Security Policy

- Connexion Developments Ltd requires that the most recent version of the information security policy be published and disseminated to all relevant system users (including vendors, contractors, and business partners). (PCI DSS Requirement 12.1.1)
- The Connexion Developments Ltd information security policy must be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment. (PCI DSS Requirement 12.1.2)
- The security policy must clearly define the information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities. (PCI DSS Requirement 12.1.3)

## 12.6 Security Awareness Program

- A formal security awareness program<sup>3</sup> must exist and participation is required for all employees working within the cardholder data environment. (PCI DSS Requirement 12.6.1)

## 12.8 Policies for Working with Third Party Service Providers (TPSPs)

- To conform to industry best practices, it is required that due diligence be performed before engaging with new service providers and is monitored for current service providers that store, process, or transmit cardholder data on Connexion Developments Ltd's behalf. Service providers, which could affect the Cardholder Data, are also in-scope of this policy.
  - Connexion Developments Ltd shall maintain a documented list<sup>4</sup> of all applicable service providers in use and the services they provide. (PCI DSS Requirement 12.8.1)
  - A written agreement with all applicable service providers is required and must include an acknowledgement of the service providers' responsibility for securing all cardholder data they receive from or on behalf of Connexion Developments Ltd, or to the extent that they could affect the security of a cardholder data environment (PCI DSS Requirement 12.8.2). In addition, the service provider must agree to provide compliance validation evidence on an annual basis. (PCI DSS Requirement 12.8.4). Prior to engaging with an applicable service provider, a thorough due diligence process<sup>5</sup> should be followed. (PCI DSS Requirement 12.8.3)
  - Connexion Developments Ltd shall review the PCI DSS attestation of compliance form(s) for its third-party service providers and confirm that the third-party service providers are PCI DSS compliant for the service being used by Connexion Developments Ltd. (PCI DSS Requirement 12.8.4)
  - Connexion Developments Ltd shall maintain a list<sup>6</sup> of which PCI DSS requirements are managed by each service provider, which are managed by Connexion Developments Ltd, and any that are shared between the service provider and Connexion Developments Ltd. (PCI DSS Requirement 12.8.5)

## 12.10 Incident Response Plan Policies

Incidents or suspected incidents regarding the security of the Cardholder Data Environment or cardholder data itself must be handled quickly and in a controlled, coordinated and specific manner. An incident response plan (IRP) must be developed and followed in the event of a breach or suspected breach. The following policies specifically address the Connexion Developments Ltd IRP<sup>7</sup>:

- Connexion Developments Ltd must maintain a documented IRP and be prepared to respond immediately to a system breach. (PCI DSS Requirement 12.10)
- The IRP must clearly define roles and responsibilities for response team members. (PCI DSS Requirement 12.10.1)
- The IRP must define contact/communication strategies to be used in the event of a compromise including

---

<sup>3</sup> See the *Security Awareness Training Process* document.

<sup>4</sup>

<sup>5</sup> See the *Service Provider Compliance Validation Process* document.

<sup>6</sup> See the *Service Provider Compliance Validation Process* document.

<sup>7</sup> See the *Incident Response Plan* document.

notification of payment brands. (PCI DSS Requirement 12.10.1)

- The IRP must define specific incident response procedures to be followed for different types of incidents. (PCI DSS Requirement 12.10.1)
- The IRP must document business recovery and continuity procedures. (PCI DSS Requirement 12.10.1)
- The IRP must detail all data backup processes. (PCI DSS Requirement 12.10.1)
- The IRP must contain an analysis of all legal requirements for reporting compromises of cardholder data (for example, California Bill 1386 which requires notification of affected consumers in the event of an actual or suspected compromise of California residents' data). (PCI DSS Requirement 12.10.1)
- The IRP must address coverage and responses for all critical system components. (PCI DSS Requirement 12.10.1)
- The IRP must include or reference the specific incident response procedures from the payment brands. (PCI DSS Requirement 12.10.1)

## Appendix A – Management Roles and Responsibilities

### Assignment of Management Roles and Responsibilities for Security

As required by policy in Section 12.5 of this security policy, the following table contains the assignment of management roles for security processes.

Table A1 - Management Security Responsibilities

Name of Role, Group, or Department	Date Assigned	Description of Responsibility
Michael Freye, Director	29-07-24	Establish, document, and distribute security policies
Michael Freye, Director	29-07-24	Monitor, analyze, and distribute security alerts and information
Michael Freye, Director	29-07-24	Establish, document, and distribute security incident response and escalation policies
Michael Freye, Director	29-07-24	Administration of user accounts on systems in the cardholder data environment
Michael Freye, Director	29-07-24	Monitor and control all access to cardholder data

Appendix B – Agreement to Comply

## Agreement to Comply with Information Security Policies

All employees working with cardholder data must submit a signed paper copy of this form. Connexion Developments Ltd management will not accept modifications to the terms and conditions of this agreement.

MICHAEL FREYE\_\_\_\_\_

Employee's Printed Name

DIRECTOR\_\_\_\_\_

Employee's Department

01454 334 990\_\_\_\_\_

Employee's Telephone Number

Unit 3, Rainbow Court, ArmstronG Way, Yate, Bristol, BS37 5NG, mike@solenoid-valves.com

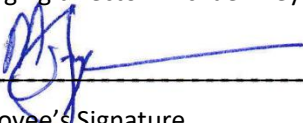
Employee's Physical Address and Mail Location

I, the user, agree to take all reasonable precautions to assure that Connexion Developments Ltd internal information, or information that has been entrusted to Connexion Developments Ltd by third parties, such as customers, will not be disclosed to unauthorized persons. At the end of my employment or contract with Connexion Developments Ltd, I agree to return to Connexion Developments Ltd all information to which I have had access as a result of my position with Connexion Developments Ltd. 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 Connexion Developments Ltd manager who is the designated information owner.

I have access to a copy of the Connexion Developments Ltd Information Security Policies Manual, I have read and understand the manual, and I understand how it affects my job. As a condition of continued employment at Connexion Developments Ltd, I agree to abide by the policies and other requirements found in that manual. I understand that non-compliance will be cause for disciplinary action up to and including system privilege revocation, dismissal from Connexion Developments Ltd, and perhaps criminal and/or civil penalties.

I agree to choose a difficult-to-guess password as described in the Connexion Developments Ltd Information Security Policies Manual, 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 company managing director Michael Freye.

  
\_\_\_\_\_

Employee's Signature