

Information Security & PCI DSS Compliance Policy

Company: Connexion Developments Ltd

Standards Referenced: PCI DSS v4.0, UK GDPR, ISO 9001:2015, ISO 14001:2015

Issue Date: January 2026

Review Cycle: Annual or upon significant business change

1. Purpose

Connexion Developments Ltd is committed to protecting the confidentiality, integrity, and availability of information assets and payment-related data. This policy sets out our approach to information security and confirms our compliance with the **Payment Card Industry Data Security Standard (PCI DSS v4.0)**.

The purpose of this policy is to provide assurance to customers, partners, and stakeholders that appropriate controls are in place to protect information and to support secure electronic commerce operations.

2. Scope

This policy applies to:

- All employees and directors of Connexion Developments Ltd
- Temporary staff, contractors, and third parties acting on our behalf
- All information systems, networks, applications, and data relevant to company operations

This policy covers environments assessed under **PCI DSS SAQ A and SAQ B**, as applicable to the company's payment processing arrangements.

3. Information Security Principles

Connexion Developments Ltd applies the following core information security principles:

- **Confidentiality:** Information is accessible only to authorised individuals
- **Integrity:** Information is accurate, complete, and protected from unauthorised modification
- **Availability:** Information and systems are available when required for legitimate business use

These principles underpin all information security controls and operational practices.

4. PCI DSS Compliance Statement

Connexion Developments Ltd confirms that:

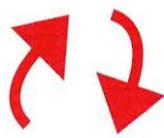
- Payment card transactions are processed using **PCI DSS-compliant third-party payment service providers**
- The company **does not store, process, or transmit cardholder data** on its own systems beyond what is permitted under applicable SAQ classifications
- PCI DSS compliance is maintained in line with **SAQ A and SAQ B** requirements, as applicable
- Compliance is reviewed annually and supported by appropriate documentation and evidence

5. Security Controls

Appropriate technical and organisational measures are implemented to protect information and payment-related environments, including:

- Secure system configuration and access controls
- Network security measures such as firewalls and endpoint protection
- Regular patching and system updates
- Use of reputable, compliant hosting and payment service providers
- Segregation of systems where appropriate
- Secure handling and disposal of information assets

Controls are proportionate to risk and reviewed periodically.



6. Vulnerability Management and Monitoring

Connexion Developments Ltd undertakes ongoing security monitoring to support PCI DSS compliance and reduce the risk of compromise.

This includes:

- **Quarterly external vulnerability scanning** by an Approved Scanning Vendor (ASV)
- Review and remediation of identified vulnerabilities where applicable
- Monitoring of security alerts and system integrity

7. Data Protection and Privacy

Personal data is processed in accordance with:

- The **UK General Data Protection Regulation (UK GDPR)**
- The **Data Protection Act 2018**

This policy operates alongside the company's **Data Protection & Information Security Policy** and **Privacy Policy**, which set out how personal data is handled and protected.

8. Incident Management

Any actual or suspected information security incident, including those relating to payment systems, must be reported immediately to management.

Incidents are:

- Assessed promptly
- Investigated proportionately
- Managed in accordance with internal procedures

Where required, incidents are reported to relevant authorities, payment providers, or affected parties.

9. Roles and Responsibilities

Management

Management is responsible for:

- Ensuring this policy is implemented and maintained
- Overseeing PCI DSS compliance and information security controls
- Reviewing security risks and mitigation measures

Employees and Others

All individuals covered by this policy are responsible for:

- Following information security procedures
- Protecting access credentials and systems
- Reporting security concerns or incidents promptly

10. Training and Awareness

Appropriate information security awareness and guidance is provided to employees relevant to their role and responsibilities.

11. Policy Review

This policy will be reviewed annually or following significant changes to:

- Payment processing arrangements
- Information systems or infrastructure
- Regulatory or PCI DSS requirements

Approved by:

Managing Director

For and on behalf of Connexion Developments Ltd