PaperWorks Online Ltd. - Payment Data Security / PCI Compliance Policy

Policy Version: 1.0
Effective Date: [Date]
Review Date: Annually, or after significant changes to payment infrastructure
Policy Owner: IT/System Administrator
PCI DSS Compliance Officer: CEO
Approved By: [CEO Name]

1.0 Purpose and Objectives

The purpose of this policy is to establish the security requirements and procedures for protecting payment card data in accordance with the Payment Card Industry Data Security Standard (PCI DSS). The primary objectives are:

- To maintain a secure environment for any interaction with cardholder data (CHD).
- To strictly limit the company's PCI DSS scope by ensuring PaperWorks Online Ltd. never stores, processes, or transmits cardholder data on its internal systems.
- To define responsibilities for ensuring ongoing compliance with PCI DSS.
- To protect the company from financial loss, reputational damage, and legal liability associated with payment card breaches.

2.0 Scope

This policy applies to:

- All Personnel: Employees, contractors, and consultants who design, manage, or have access to systems involved in payment processing.
- All Systems: Any system, network, or component that is connected to or could impact the security of the Cardholder Data Environment (CDE), including the public-facing website, checkout system, and administrative panels.
- Third-Party Service Providers: Any vendor involved in payment processing (e.g., Payment Gateway, hosting provider).

3.0 Policy Statement

PaperWorks Online Ltd. is committed to processing payment card transactions securely and in full compliance with the PCI DSS. The company's strategy is based on scope reduction: we outsource all payment card processing to a PCI DSS Level 1 compliant Third-Party Payment Service Provider (PSP). Our internal systems are designed to never come into contact with primary account numbers (PAN), sensitive authentication data (SAD), or full magnetic stripe data.

4.0 Definitions

- Cardholder Data (CHD): The full Primary Account Number (PAN) along with any of the following: cardholder name, expiration date, service code. Sensitive Authentication Data (SAD) includes full track data, CAV2/CVC2/CVV2/CID, and PINs.
- Cardholder Data Environment (CDE): The people, processes, and technology that store, process, or transmit cardholder data. For PaperWorks, our CDE is explicitly defined as the systems of our approved PCI DSS Level 1 Payment Service Provider.
- Payment Service Provider (PSP): The third-party company (e.g., Stripe, PayPal) certified to PCI DSS Level 1 that provides the payment gateway and processing services.
- SAQ A: The PCI DSS Self-Assessment Questionnaire A, applicable to merchants who have fully outsourced all cardholder data functions.

5.0 Roles and Responsibilities

- CEO / Management: Ultimate responsibility for PCI DSS compliance, providing resources, and approving this policy.
- IT/System Administrator: Responsible for the technical implementation of this policy, managing integration with the PSP, ensuring system security, and maintaining evidence for compliance.
- All Employees: Responsible for understanding and adhering to this policy, especially regarding the prohibition of manually recording or handling full card numbers.

6.0 Technical and Operational Requirements

6.1 Payment Processing Model

- 6.1.1 All payment card transactions must be processed directly through the approved PCI DSS Level 1 Payment Service Provider (PSP).
- 6.1.2 The company website checkout must use either:
    - A redirect to the PSP's secure hosted payment page.
    - An iFrame/embedded form served directly from the PSP's domain.
- 6.1.3 Under no circumstances shall cardholder data be entered into, transmitted through, or stored on any internal PaperWorks system (e.g., web server, database, email, support tickets, paper forms).

6.2 Security of Systems Connected to the CDE

Although CHD does not touch our systems, systems that redirect to the CDE must be secured:

- 6.2.1 Network Security: A Web Application Firewall (WAF) must be deployed in front of the public website. Internal administrative networks must be firewalled.
- 6.2.2 Encryption: All public-facing pages, especially checkout initiation pages, must use strong cryptography (TLS 1.2 or higher) with valid certificates.
- 6.2.3 Vulnerability Management: All systems (web server, CMS, plugins) must be kept up-to-date with the latest security patches. A process for quarterly vulnerability scanning of external-facing IPs will be maintained.

- 6.2.4 Access Control: Access to website administrative functions and hosting panels must be protected by strong, unique passwords and Multi-Factor Authentication (MFA).
- 6.2.5 Logging & Monitoring: Audit logs for administrative access and security events must be enabled and reviewed weekly.

6.3 Data Retention and Handling

- 6.3.1 The company may only store, for business purposes, the last four digits of the PAN, the card brand, and the expiration date, as provided by the PSP.
- 6.3.2 Paper records containing any cardholder data are strictly prohibited. If received accidentally (e.g., a faxed order), they must be securely destroyed (cross-cut shredding) immediately upon identification.
- 6.3.3 Employees are forbidden from asking customers to send card details via email, chat, or phone for the purpose of payment.

6.4 Third-Party Management

- 6.4.1 The relationship with the PSP must be governed by a formal agreement that acknowledges the PSP's responsibility for securing cardholder data.
- 6.4.2 Annual confirmation of the PSP's PCI DSS Level 1 certification (Attestation of Compliance) must be obtained and filed by the IT Administrator.

6.5 Incident Response

- 6.5.1 Any suspected loss, theft, or unauthorized disclosure of payment card data must be reported immediately to the CEO and IT Administrator.
- 6.5.2 The company's Incident Response & Breach Notification Policy will be followed. This includes notifying the PSP and, if a breach is confirmed, following mandated card brand reporting procedures.

7.0 Compliance Validation

- 7.1 Annually, the CEO or designated officer will complete the PCI DSS Self-Assessment Questionnaire SAQ A.
- 7.2 The IT Administrator will maintain documentation necessary for the SAQ A, including:
    - Evidence of the PSP's current PCI DSS compliance.
    - Records of security patch management.
    - WAF and vulnerability scan reports.
    - Policy review and employee training records.

8.0 Training and Awareness

- All relevant personnel will receive annual training on this policy, focusing on the importance of PCI DSS, the "do not store" principle, and how to identify and report suspected security incidents.

9.0 Policy Compliance and Enforcement

- Non-compliance with this policy will result in disciplinary action, up to and including termination of employment and potential legal action.
- Compliance with this policy will be verified through audits, log reviews, and management oversight.

10.0 Related Documents

- Information Security Policy
- Access Control Policy
- Incident Response & Breach Notification Policy
- Data Protection & Privacy Policy (GDPR)
- Record of Processing Activities (ROPA)
- Agreement with Payment Service Provider

Review and Acknowledgment
This policy shall be reviewed annually. All personnel with access to systems involved in the payment process must read and acknowledge this policy.
Employee/Contractor Acknowledgment
I, [Employee Name], have read, understood, and agree to comply with the PaperWorks Online Ltd. Payment Data Security / PCI Compliance Policy.
Signature: _____
Date: _____
For Company Use:
Date Provided: _____
Acknowledgment Copy Filed: [ ]