PaperWorks Online Ltd. - Information Security & Compliance Policy Suite

1. Company Overview

- Company Name: PaperWorks Online Ltd.
- Address: 123 Stationery Ave, Dublin, Ireland
- Mission Statement: “Deliver high-quality, sustainable paper products to customers with convenience and excellent service.”
- Business Description: A small e-commerce retailer selling paper and stationery via an online store. The business operates within the EU, serving EU customers, and processes personal data and card payments through a secure, PCI-compliant third-party gateway.

---

2. Core Security & Compliance Policies

2.1. Information Security Policy

Policy Owner: CEO/Administrator

Purpose: To establish management’s commitment to information security, define security objectives, and assign responsibilities to protect the confidentiality, integrity, and availability of company information assets.

Key Provisions:

- Management endorses a culture of security and provides necessary resources.
- Security objectives align with business goals and legal/regulatory requirements (GDPR, PCI DSS).
- All employees are responsible for adhering to security policies.

- The policy is reviewed annually or after significant changes.

2.2. Access Control Policy

Policy Owner: IT/System Administrator

Purpose: To ensure that access to information and systems is restricted to authorized individuals based on the principle of least privilege.

Key Provisions:

- Individual Accounts: Unique user accounts for all staff; shared/generic accounts are prohibited.
- Authentication: Strong passwords (min. 12 chars, complexity) are mandatory. Multi-Factor Authentication (MFA) is required for all administrative access and cloud management consoles.
- Role-Based Access Control (RBAC): Privileges are assigned based on predefined roles (see Section 3).
- Reviews: Access rights are reviewed quarterly. Accounts are disabled immediately upon termination.

2.3. HR/Personnel Security Policy

Policy Owner: CEO/Manager

Purpose: To mitigate risks from human error, fraud, or misuse by defining security practices throughout the employment lifecycle.

Key Provisions:

- Pre-employment: Role-dependent background checks and signed confidentiality agreements.
- Onboarding: Mandatory security awareness and role-specific training.
- Employment: Ongoing security training; reinforcement of Acceptable Use Policy.
- Termination: Formal exit process ensuring prompt revocation of all physical and logical access.

2.4. Acceptable Use Policy (AUP)

Policy Owner: IT/System Administrator

Purpose: To define the acceptable use of company IT assets, including computers, networks, email, and internet access.

Key Provisions:

- Company systems are for business purposes.
- Prohibition of illegal activities, copyright infringement, and accessing inappropriate material.
- Employees must not install unauthorized software.
- Guidelines for secure remote work and use of personal devices (if permitted).

2.5. Data Protection & Privacy Policy (GDPR)

Policy Owner: CEO/Data Protection Lead

Purpose: To ensure the lawful, fair, and transparent processing of personal data in compliance with the GDPR.

Key Provisions:

- Lawful Basis: Data is processed under contract (order fulfillment) or explicit consent (marketing).
- Data Minimization: Only necessary data is collected and retained.
- Individual Rights: Procedures to address Data Subject Access Requests (DSARs) within one month.
- Records: Maintenance of a Record of Processing Activities (ROPA).
- External Notice: A Privacy Notice is published on the website, detailing data practices.

2.6. Payment Data Security / PCI Compliance Policy

Policy Owner: IT/System Administrator

Purpose: To ensure the secure handling of payment card data and maintain compliance with PCI DSS requirements.

Key Provisions:

- Scope Reduction: Cardholder data (CHD) is never stored, processed, or transmitted on internal systems. All payments are handled via a PCI DSS Level 1 compliant third-party gateway using hosted payment pages/iFrames.
- Segregation: The cardholder data environment (CDE) is limited to the third-party gateway.
- Internal Controls: Systems redirecting to the gateway are protected by firewalls, kept patched, and use strong encryption (TLS 1.2+).
- Compliance Validation: The company will annually complete the PCI DSS Self-Assessment Questionnaire SAQ A.

2.7. Incident Response & Breach Notification Policy

Policy Owner: CEO/Incident Response Lead

Purpose: To establish a framework for detecting, responding to, and recovering from security incidents, including mandatory breach reporting.

Key Provisions:

- Definition & Classification: Definitions of security events and incidents.
- Response Team: Designated team with clear roles (Lead, IT, Communications).
- Procedure: Steps for Identification, Containment, Eradication, Recovery, and Lessons Learned.
- Notification: Process to report qualifying personal data breaches to the Data Protection Commission (DPC) within 72 hours and to affected data subjects without undue delay, as per GDPR Article 33/34.

2.8. Business Continuity & Disaster Recovery Policy

Policy Owner: CEO/Manager

Purpose: To ensure the continuity of critical business operations and the recovery of IT systems following a disruption.

Key Provisions:

- Backup Policy: Critical data (website, databases, customer orders) is backed up daily. Backups are stored encrypted both on-site and in a secure, off-site/cloud location. Restoration is tested quarterly.
- Recovery Objectives: Defines target Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for key systems.
- Plan Activation: Procedures for declaring a disaster and activating the recovery plan.

2.9. Logging & Monitoring Policy

Policy Owner: IT/System Administrator

Purpose: To detect, investigate, and respond to security events through the generation, retention, and review of audit logs.

Key Provisions:

- Log Generation: Enable logging for all user access (success/failure), admin actions, system errors, and firewall activity.
- Log Protection: Logs are stored centrally, protected from tampering, and retained for at least one year (or as required by PCI DSS).
- Log Review: Automated alerting for critical events (e.g., multiple failed logins). Regular manual review performed weekly.

---

3. User Account List & Role Definitions

Username	Role	Access Privileges (Least Privilege)	MFA Enforced?
Michael	CEO / System Admin	Full administrative access to website CMS, database, cloud infrastructure, and financial reports.	Yes
Pam	IT / System Admin	Admin access to technical infrastructure, backup systems, and user account management. No direct access to financial data.	Yes
Alice	Sales & Customer Service	Read/write access to customer order management system and CRM. No access to server administration or raw database.	Recommended
James	Inventory & Fulfillment	Read/write access to inventory/product database and shipping logistics. Read-only access to related orders.	No

(Contractor)	Web Developer	Temporary, limited access to development/staging environment only. Logs all activity.	Yes

---

4. Technical & Operational Controls Summary

- Webstore Platform: Secure e-commerce platform (e.g., Shopify, WooCommerce on managed hosting) kept updated.
- Payment Gateway: Integrated PCI DSS Level 1 compliant gateway (e.g., Stripe, PayPal). Configuration: Hosted payment page/iFrame to ensure CHD never touches our servers.
- Encryption:
  - In Transit: TLS 1.2+ (HTTPS) enforced across entire site.
  - At Rest: Full-disk encryption on servers; database fields containing personal data encrypted.
- Network Security: Web Application Firewall (WAF) in front of website. Network firewall segregating internal office network.
- Endpoint Security: Antivirus/anti-malware on all company-owned workstations.
- Backups: Automated daily backups of website and databases. Encrypted backups stored both locally and with a cloud provider (e.g., AWS S3, Backblaze). Test restore performed quarterly.
- Website Documentation: Public-facing Privacy Notice, Terms of Service, and Cookie Consent banner (GDPR compliant) are present and current.
- Vendor Management: Data Processing Agreements (DPAs) in place with key vendors (hosting, payment gateway, email service).

---

5. Defined Compliance Scopes

5.1. PCI DSS Scope

- In-Scope (Cardholder Data Environment - CDE): The third-party Payment Gateway and its hosted payment pages. The company's website redirects to this gateway but does not transmit, process, or store CHD.
- Out-of-Scope: Internal company servers, databases, and workstations, as they have no connectivity to or interaction with CHD.
- Compliance Pathway: SAQ A (for merchants using a fully outsourced, PCI-validated payment solution).

5.2. GDPR Scope

- In-Scope Data: All personal data of EU-based customers and employees. This includes names, addresses, email, phone numbers, order history, IP addresses, and any correspondence.
- In-Scope Systems & Processes: The website, order database, CRM, email marketing system, HR files, and any physical records.
- Key Obligations: Lawful processing, data minimization, security, breach notification, honoring data subject rights, maintaining ROPA.

5.3. ISO 27001 (Informal Alignment) Scope Statement

- The Information Security Management System (ISMS) applies to:
    - The design, operation, and maintenance of the PaperWorks Online Ltd. e-commerce store (www.paperworksonline.ie).
    - All associated information assets required for its operation, including the customer/order database, inventory system, and internal corporate IT systems.
    - All employees, contractors, and third-party vendors who access, process, or manage these in-scope assets.
    - The primary location at 123 Stationery Ave, Dublin, and any approved remote work locations.
- Objective: To ensure the confidentiality, integrity, and availability of information critical to the business's mission of serving its customers.

Document Approval:

Michael, CEO

Date: [Date of Implementation]

Review Cycle: All policies are to be reviewed annually or following significant security incidents or business changes.