PaperWorks Online Ltd. - Information Asset Inventory

Document Version: 1.0
Last Updated: [Date]
Asset Owner: CEO/Manager
Maintained By: IT/System Administrator
Review Frequency: Quarterly, or upon significant change

1.0 Purpose

This document provides a comprehensive inventory of PaperWorks Online Ltd.'s information assets. Maintaining an accurate asset inventory is critical for:

- Implementing appropriate security controls based on asset value and sensitivity.
- Supporting risk assessment and management activities.
- Fulfilling compliance requirements for PCI DSS, GDPR, and ISO 27001.
- Enabling effective incident response and business continuity planning.

2.0 Scope

This inventory covers all information assets owned, leased, or managed by PaperWorks Online Ltd. that are used in the course of business, including physical hardware, software, data, and third-party services.

3.0 Asset Classification Scheme

All assets are classified based on their confidentiality, integrity, and availability (CIA) requirements:

Classification	Description	Examples	Handling Requirements
RESTRICTED	Highly sensitive. Unauthorized disclosure/alteration would cause severe damage.	Full Payment Card Data, System Admin Credentials	Strong encryption, strict access controls (MFA), detailed logging. Never stored unless absolutely necessary.

CONFIDENTIAL	Sensitive internal or customer data. Disclosure/alteration would cause significant harm.	Customer PII (name, address, email, phone), Employee HR records, Financial reports	Encryption at rest and in transit, role-based access, secure disposal.
INTERNAL	Business internal data not for public disclosure. Unauthorized disclosure would cause moderate harm.	Internal procedures, non-sensitive operational data, inventory wholesale costs	Access limited to employees, standard security controls.
PUBLIC	Information approved for public release.	Marketing website content, published product descriptions, public blog posts	Standard web security (HTTPS), integrity checks.

4.0 Asset Inventory Register

4.1 Hardware Assets

Asset ID	Asset Name / Description	Location	Owner / Custodian	Classification	Criticality	Notes / Serial Number
HW-001	Primary Office Server (if applicable)	Office Server Room / Hosting DC	IT Admin	Internal	High	Virtual Machine on Cloud Provider.
HW-002	CEO Laptop - Dell XPS 15	Office / Remote	CEO	Confidential	High	Encrypted (BitLocker), SN: ABC123XYZ
HW-003	IT Admin Laptop - MacBook Pro	Office / Remote	IT Admin	Confidential	High	Encrypted (FileVault), SN: DEF456UVW

HW-004	Sales Workstation 1 - Desktop PC	Office, Sales Desk	Alice (Sales)	Internal	Medium	Standard user account, antivirus.
HW-005	Inventory Workstation - Laptop	Office / Warehouse	James (Inventory)	Internal	Medium	SN: GHI789RST
HW-006	Office Network Router/Firewall	Office Network Rack	IT Admin	Internal	High	Model: Ubiquiti Dream Machine
HW-007	Office Network Switch	Office Network Rack	IT Admin	Internal	Medium	8-port managed switch
HW-008	Office Multifunction Printer	Main Office	IT Admin	Internal	Low	Configured with secure print.
HW-009	Company Mobile Phone (CEO)	With CEO	CEO	Confidential	Medium	Used for 2FA and business comms.

4.2 Software & Application Assets

Asset ID	Asset Name / Description	Type / Vendor	Hosting Location	Owner	Data Classification	License Key / Version
SW-001	E-commerce Website Platform (e.g., Shopify/WooCommerce)	SaaS / Custom App	Cloud (EU Region)	IT Admin	Varies by data	SaaS Subscription.
SW-002	Customer & Order Database	Database	Cloud (Private Subnet, EU)	IT Admin	Confidential	v14.2, encrypted at rest.

	(MySQL/PostgreSQL)					
SW-003	Product/Inventory Management System	Integrated Module / SaaS	Cloud	IT Admin	Internal	Part of e-commerce platform.
SW-004	Payment Gateway Integration (Stripe SDK)	Library/API Connector	Web Server	IT Admin	Internal	Latest stable version.
SW-005	Corporate Email (Google Workspace / Microsoft 365)	SaaS	Cloud	CEO	Confidential	5-user subscription.
SW-006	Endpoint Antivirus (e.g., Bitdefender GravityZone)	Commercial Software	All Workstations	IT Admin	Internal	Company license.
SW-007	Backup & Recovery Software (e.g., Veeam/Cloud Backup)	Commercial Software	Cloud & Local	IT Admin	Confidential	License: BKP-2024-001
SW-008	Accounting Software (e.g., Xero)	SaaS	Cloud	CEO	Confidential	Subscription.
SW-009	VPN Client (for remote admin access)	Commercial Software	Admin Workstations	IT Admin	Internal	Part of firewall solution.

SW-010	Operating Systems (Windows 11 Pro, macOS)	Commercial OS	Workstations	IT Admin	Internal	Licensed per device.

4.3 Information & Data Assets

Asset ID	Data Set Description	Format / Storage Location	Data Owner	Classification	Retention Period	Contains PII? (GDPR)
DA-001	Customer Personal Data (Name, Address, Email, Phone)	Database Table customers	CEO	Confidential	7 years (legal/financial)	Yes
DA-002	Order History & Transaction Data	Database Table orders	CEO	Confidential	7 years	Yes (linked to DA-001)
DA-003	Payment Tokens & Last 4 Digits PAN	Database Table payments	CEO	Confidential	7 years	Yes (limited)
DA-004	Product Catalogue & Inventory Data	Database Table products	IT Admin	Internal	Indefinitely (active)	No
DA-005	Employee HR Records & Contracts	Encrypted Cloud Storage (Google Drive)	CEO	Confidential	7 years post-employment	Yes
DA-006	Financial Records & Invoices	Accounting Software (Xero)	CEO	Confidential	7 years	Yes (supplier/customer)

DA-007	Website Backups (Full System)	Encrypted Cloud Storage (Backblaze B2)	IT Admin	Confidential	30 days rolling, 12 month archive	Yes (contains DA-001/002)
DA-008	System Logs & Audit Trails	Centralized Log Server / Cloud	IT Admin	Internal	1 year (PCI DSS min.)	Yes (IP addresses)
DA-009	Marketing Mailing List	Email Marketing Platform (Mailchimp)	CEO	Confidential	Until unsubscribe	Yes

4.4 Third-Party Service Assets (Vendors)

Asset ID	Service Provider	Service Provided	Data Shared	Owner	Criticality	Contract/ DPA in Place?
TP-001	Cloud Hosting Provider (e.g., AWS, Shopify)	Infrastructure / Platform	All business data	IT Admin	Critical	Yes, DPA & Terms
TP-002	Payment Service Provider (e.g., Stripe)	Payment Processing	Payment Tokens, Order Value	CEO	Critical	Yes, PCI DSS Level 1
TP-003	Domain Registrar & DNS Provider	Domain Management, DNS	None	IT Admin	High	Yes (Terms)
TP-004	Email Service Provider (Google/Microsoft)	Corporate Email & Collaboration	Employee & Customer PII	CEO	High	Yes, DPA

TP-005	Shipping & Logistics Partner (e.g., An Post)	Order Fulfillment	Customer Address, Phone	Sales Lead	High	Yes (Data Agreement)
TP-006	Backup Storage Provider (e.g., Backblaze)	Off-site Encrypted Backups	Encrypted business data	IT Admin	High	Yes, Terms of Service
TP-007	Web Security Provider (WAF, CDN)	DDoS Protection, WAF	Web traffic logs	IT Admin	Medium	Yes
TP-008	Accounting Software Provider (Xero)	Financial Management	Financial records, invoices	CEO	Medium	Yes, DPA

4.5 Physical Media & Documentation

Asset ID	Description	Location	Custodian	Classification	Disposal Method
PM-001	Paper Customer Orders (if received)	Locked Filing Cabinet (Office)	Sales Lead	Confidential	Cross-cut shredding
PM-002	Employee Personnel Files	Locked Filing Cabinet (CEO Office)	CEO	Confidential	Cross-cut shredding
PM-003	Backup Tapes/External HDDs (if used)	Fireproof Safe & Off-site	IT Admin	Confidential	Secure degaussing & destruction
PM-004	Network Configuration Documentation	Password Manager & Secure Cabinet	IT Admin	Internal	Secure shredding

5.0 Responsibilities & Maintenance

- Asset Owners (Listed in Inventory): Responsible for classifying their assets, approving access, and defining protection requirements.
- IT Administrator: Responsible for maintaining this inventory, updating it upon changes, and implementing technical controls as defined.
- All Employees: Responsible for reporting any new, unaccounted, or decommissioned assets to the IT Administrator.

Update Procedure:

1. Any new asset acquisition must be registered in this inventory within 5 business days.
2. Assets being decommissioned must be securely erased/disposed of and marked as "Retired" in the inventory, with a disposal record.
3. This master inventory is reviewed and verified quarterly by the IT Administrator and CEO.

6.0 Related Documents

- Information Security Policy
- Access Control Policy
- Data Protection & Privacy Policy (GDPR)
- Asset Disposal Procedure
- Vendor Management Policy

Document Approval

This asset inventory has been reviewed and approved.

CEO Signature: ___________________________

Date: ___________________________

IT Administrator Signature: ___________________________

Date: ___________________________