ACCESS CONTROL POLICY

PaperWorks Online Ltd.

Version 1.0 – 24 December 2025

Approved by: Michael Byrne (CEO)

Next review: 24 June 2026

1. PURPOSE
   To ensure that only authorised, authenticated individuals can access PaperWorks information systems and data, and that they are granted the minimum rights necessary to fulfil their role (least-privilege).
2. SCOPE
   All logical access to:

- Production web server, database, back-office applications
- Cloud consoles (hosting, DNS, e-mail, backups)
- Third-party services that hold company or customer data (Stripe, G-Suite, Shopify, etc.)
- Corporate laptops, mobiles, and any device that stores or caches customer data
  Applies to all employees, contractors, third-party support staff and test accounts.

3. OBJECTIVES
   a) Prevent unauthorised access to personal data (GDPR Art. 32).
   b) Restrict card-holder data environment (CDE) to essential personnel only (PCI DSS Req. 7 & 8).
   c) Provide timely revocation when employment or contract ends.
   d) Maintain an auditable access trail for certification and forensic purposes.
4. ROLES & RESPONSIBILITIES
   Role (example users) – Data/Systems – Justification

- CEO / Owner (Michael) – Full admin (all systems) – Business continuity
- IT / System Admin (Pam) – Super-admin (servers, DB, backups) – Daily ops & security
- Sales & CS staff (Alice, John) – CRM, order DB (read/write own customers) – Core duties
- Inventory clerk (James) – Product DB (read/write stock) – Stock control
- External accountant – Finance folder (read-only) – Statutory accounts

- Web developer (contract) – Source-code repo (read-only main, no prod DB) – Maintenance
- PCI auditor – CDE segment (read-only logs) – Compliance validation

5. USER REGISTRATION & APPROVAL
6. Line manager raises “User Access Request” (UAR) form (Google sheet / ticket).
7. Data Owner (Michael for prod, Pam for infra) approves in writing.
8. IT creates individual account; default password 16-char generated.
9. User must change password on first log-in and enrol MFA within 24 h.
10. Account details entered in central “Access Register” (Airtable) with: name, role, systems, approver, creation date.
11. AUTHENTICATION STANDARDS

- Password length ≥ 12 characters, complexity 3/4 classes, 90-day expiry (PCI), no reuse of last 5.
- Multi-Factor Authentication (TOTP or WebAuthn) enforced for:
  – All admin / privileged accounts
  – All remote access (VPN, SSH, RDP, cloud console)
  – All CDE access (PCI DSS Req. 8.3)
- Account lockout after 5 failed attempts in 15 min; alert sent to IT.
- Single Sign-On used where supported; separate SSO tenant for production vs dev.

7. PRIVILEGED ACCESS MANAGEMENT (PAM)

- Shared root / admin passwords stored only in Bitwarden org vault; checkout logged.
- SSH keys for prod servers: passphrase-protected, unique per admin, 4096-bit RSA min.
- Interactive admin sessions logged (script + tty) to Graylog; logs retained 1 year.
- No privileged access from portable devices unless full-disk-encrypted & AV up-to-date.

8. AUTHORISATION & LEAST-PRIVILEGE

- RBAC groups mirror the role list (§4).
- Default “deny-all”; rights added only for required business function.
- Write access to customer personal data limited to Sales & CS; delete right reserved for CEO & DPO.
- No production data used in development / test.
- SQL database: separate DB roles; no direct table access for web user—stored procedures only.

9. REVIEW & RECERTIFICATION

- Quarterly “Access Review” run by Pam: export Access Register → managers confirm → disable obsolete accounts.
- After each review, evidence (screenshots, sign-offs) saved in ISO 27001 folder.

- Any privilege escalation ticket automatically expires after 72 h unless re-approved.

10. CHANGES & TEMPORARY ACCESS

- Emergency change (e.g. outage) may be granted verbally by CEO, but must be logged in incident ticket within 1 h and retro-approved within 24 h.
- Temporary accounts (contractors, interns) given fixed expiry date; system auto-disables.

11. TERMINATION OR ROLE CHANGE

- HR e-mails “Leaver Form” to IT on last working day at latest.
- IT disables all accounts, revokes SSH keys, removes from MFA, changes any shared credentials user had access to, and updates Access Register.
- Evidence of revocation stored in personnel file.

12. REMOTE & THIRD-PARTY ACCESS

- VPN IP-whitelist + certificate + MFA; no split-tunnelling.
- Third-party support given time-bound account only; activity screen-recorded.
- Data Processing Agreement must be signed before external access to personal data.

13. MONITORING & LOGGING

- All authentication events (success & fail) sent to Graylog; alerts for:
  – Multiple failed logins
  – Log-in outside business hours (admin)
  – New device / geo-impossible travel
- Logs retained ≥ 1 year (PCI DSS 10.3) and protected against tampering (WORM backup).

14. NON-COMPLIANCE & SANCTIONS
    Violation of this policy may result in suspension of access and disciplinary action up to termination. Serious cases (data breach) will be reported to the Data Protection Commission within 72 h.

15. AWARENESS & TRAINING
    Policy included in onboarding pack; staff must sign acknowledgement. Annual refresher training covers phishing, password hygiene, and secure remote work.

16. DOCUMENT CONTROL
    Owner: Pam Kelleher – IT Manager
    Location: …/ISMS/POL-04-Access-Control.pdf
    Revision history: inside back page.
    Supersedes: none.
    Related docs:

- Information Security Policy (POL-01)
- HR Security Policy (POL-03)

- PCI DSS Compensating Controls Matrix
- GDPR Record of Processing Activities (RoPA)