HR / Personnel Security Policy for PaperWorks Online Ltd.

It maps directly to ISO 27001 Annex A.7, supports GDPR “appropriate technical & organisational measures”, and can be dropped straight into the company ISMS folder.

HR / PERSONNEL SECURITY POLICY

PaperWorks Online Ltd.

Version 1.0 – 24 December 2025

Owner: HR Manager (Alice) | Approved by: CEO (Michael)

Next review: 24 June 2026

---

1. PURPOSE

Protect company and customer information by embedding security into every stage of the employment life-cycle: before, during and after employment .

---

2. SCOPE

Applies to all employees, contractors, interns, agency staff and external consultants who access PaperWorks systems, premises or data.

---

3. OBJECTIVES

- Meet ISO 27001 Annex A.7 controls .

- Satisfy GDPR “data-protection by design & default” and staff-training obligations .
- Reduce insider-threat risk (negligent or malicious) .
- Ensure rapid, documented revocation of access on termination or role change.

---

4. ROLES & RESPONSIBILITIES

TableCopy

Role	**Security responsibilities**
CEO (Michael)	Policy sponsor, disciplinary appeals
HR Manager (Alice)	Policy owner, screening, training records, leavers checklist
Line Managers	Day-to-day security behaviour, incident reporting
IT Admin (Pam)	Technical on-/off-boarding (accounts, MFA, keys)
All staff	Follow policy, complete training, report breaches

---

5. PRE-EMPLOYMENT CONTROLS

5.1 Screening (ISO A.7.1.1)

- Identity, right-to-work, reference and qualification checks for every candidate .
- Additional checks (Garda Vetting, credit check) for roles with access to card-holder data or financial systems .
- Contractors must supply evidence of equal screening or undergo ours .
- Results recorded in HR file; unsatisfactory checks = conditional offer withdrawn.

5.2 Security Clause in Contract (ISO A.7.1.2)

Every contract/offer letter contains:

- Confidentiality & non-disclosure lasting 5 years post-employment .
- Acceptable-Use, Data-Protection and ISMS policy adherence.
- Disciplinary sanctions up to dismissal for deliberate breaches.
- Return-of-assets requirement.

---

6. DURING EMPLOYMENT

6.1 Management Security Duties (ISO A.7.2.1)

- Managers include security objectives in annual performance reviews .
- Escalate any security policy violation to HR within one business day.

6.2 Security Awareness & Training (ISO A.7.2.2)

- Induction (Day 1): GDPR, phishing, password, PCI-DSS do's & don'ts.
- Quarterly micro-trainings: 10-minute video plus 3-question quiz; pass mark 80 %.
- Annual refresher: live 45-minute session; attendance recorded.
- Role-specific add-ons: developers (secure-code), sales (customer-DPIA), finance (PCI).
  Records retained in LMS > 3 years for audit evidence.

6.3 Disciplinary Process (ISO A.7.2.3)

TableCopy

Tier	Example	Sanction
1st minor	Unlocked screen	Verbal warning
2nd repeat or negligent	Sending customer list to personal e-mail	Written warning

3rd serious or wilful	PCI log disclosure, data theft	Final written warning / dismissal & legal action

Right of appeal to CEO; all outcomes filed in HR system .

6.4 Access Control Review

- HR supplies leavers/new-starter list to IT weekly.
- Line managers re-certify user rights every 6 months (evidence saved).

---

7. TERMINATION OR ROLE CHANGE (ISO A.7.3.1)

7.1 Leaver Workflow (T-48 h to last day)

1. HR raises “Leaver Ticket” in Jira.
2. IT disables accounts, revokes MFA, rotates shared credentials, removes from VPN, moves e-mail to alias.
3. Manager collects laptop, card-key, paper notebooks; signed “Asset Return” form.
4. HR reminds leaver of ongoing confidentiality & data-deletion obligations.
5. HR & IT update Access Register & Asset Inventory; ticket closed.

7.2 Internal Transfer

- Old rights revoked before new ones granted; training gap analysis completed within 5 days.

---

8. DATA PROTECTION SPECIFICS

- Employee personal data kept in encrypted HRIS; access limited to HR + CEO.
- Retention: recruitment records 6 months, payroll 6 years (ROI law).
- Cross-border HR tools (e.g. cloud-HR) covered by EU SCC Data-Processing Agreement.

---

9. DOCUMENTATION & RECORDS

TableCopy

Record	Location	Retention
Screening evidence	HR folder	Life of employment + 3 yrs
Training logs	LMS	3 yrs
Leaver check-lists	G-Drive “HR/Leavers”	3 yrs
Disciplinary outcomes	HRIS	5 yrs

---

10. COMPLIANCE & AUDIT

- Internal audit checks 10 % sample of personnel files annually.
- External ISO 27001 & PCI DSS assessments will inspect this policy plus evidence above .

---

11. AWARENESS

Policy published in Notion > HR > Security; acknowledgement required at induction and every refresh.

---

12. REVISION HISTORY

TableCopy

Version	Date	Author	Change

1.0	24-Dec-25	Alice	Initial release