INCIDENT RESPONSE & BREACH NOTIFICATION POLICY

PaperWorks Online Ltd.

Version 1.0 – 24 December 2025

Owner: Pam Kelleher (IT Admin / IRT Lead)

Approved by: Michael Byrne (CEO)

Next review: 24 June 2026

---

1. PURPOSE

Ensure that security and privacy incidents are detected, contained, eradicated and recovered quickly, and that statutory breach notifications (PCI DSS, GDPR, Irish law) are made within the required time-windows.

---

2. SCOPE

Applies to all information assets used to operate the on-line stationery store:

- Web server, database, cloud consoles, endpoints, e-mail, backups
- Offices at 123 Stationery Ave, Dublin 8
- All staff, contractors and third-party support who touch card-holder or personal data

---

3. OBJECTIVES

- Meet 72-hour GDPR and PCI DSS 12.10 notification clocks
- Minimise business downtime, reputational damage and regulatory fines
- Provide documented, repeatable steps that scale to a “major incident” (> 100 k records)

---

4. INCIDENT-RESPONSE FRAMEWORK

We adopt the 4-phase NIST model :

1. Preparation
2. Detection & Analysis
3. Containment, Eradication & Recovery
4. Post-Incident Activity

---

5. ROLES & RESPONSIBILITIES

TableCopy

Role (Name)	**Duties**
Incident Commander (IC) – Pam	Overall lead, go/no-go decisions, external comms
Security Analyst – rotating (Pam / contractor)	Log & artefact collection, forensics
Communications Officer – Michael	Media, customer, regulator statements
Legal / Privacy – Michael (acting DPO)	GDPR/PCI risk assessment, breach notices
Business Owner – Alice (Sales lead)	Impact assessment, customer-service scripts
Scribe – Google Doc (auto time-stamp)	Keeps contemporaneous decision log

If Pam is unavailable Michael becomes IC.

---

6. PHASE 1 – PREPARATION

- Incident Response Plan (this doc) & quick-reference “IR playbook” printed and in Notion
- 24×7 monitoring: CloudWatch, UptimeRobot, Stripe web-hook alerts → Slack #security
- IR jump-bag: encrypted USB, live Linux image, chain-of-custody forms, contact cards
- Annual table-top exercise (Q1) and after-hours call-tree test (Q3)
- Retained external forensics firm contract on file (24 h SLA)

---

7. PHASE 2 – DETECTION & ANALYSIS

Detection sources:

- WAF / IDS alerts, failed-login spikes, new admin users, unusual SQL queries
- Employee report (phish click, lost laptop) – report to security@paperworks.ie or Slack #security

Triage within 30 min:

1. Severity score = (Impact 1-4) × (Likelihood 1-4) – see table below
2. Classify:
    - P1-Critical – live data exfil / ransomware / root access
    - P2-High – service down > 1 h or > 500 customer records at risk
    - P3-Medium – isolated malware, failed attack
    - P4-Low – policy violation, no data impact
3. Open Jira “INC-YYYY-###” ticket – auto mirror to HHS-style log
4. Preserve evidence: snapshot disk, pull logs, note UTC time, hash files

TableCopy

Impact	Examples

4 – Catastrophic	> 100 k records, card data, media exposure
3 – High	501-100 k records, personal data, service stop
2 – Medium	< 500 records, minor PCI scope
1 – Low	no personal data, single user

---

8. PHASE 3 – CONTAINMENT, ERADICATION, RECOVERY

8.1 Containment (minutes-hours)

- Isolate affected instance / subnet – change AWS SG, disable account, rotate API keys
- Block IP at WAF, push Suricata rule
- Continue logging – do not power-off if possible (lose RAM artefacts)

8.2 Eradication (hours)

- Remove malware, delete rogue accounts, patch CVE, reset all privileged passwords & MFA seeds
- Run AV/EDR full scan; verify clean with second tool

8.3 Recovery (hours-days)

- Restore from gold-image AMIs or immutably stored backups (S3 Object Lock)
- Re-introduce to production only after sign-off by IC + Business Owner
- Monitor for 72 h “quiet period” before closing incident

---

9. BREACH-NOTIFICATION DECISION TREE

Copy

```
Suspected incident
```

```
    │
    ├─ No personal/PCI data involved → Close as "security incident only"
    │
    └─ Personal data / PCI involved → Risk Assessment (OMB-style)
[^8^][^10^]
           │
           ├─ Low risk of harm → Document reason, no external notice
           │
           ├─ Risk exists → Notify DPC within 72 h (GDPR) [^10^]
           │                    Notify Stripe / acquiring bank within 72 h
(PCI)
           │
           └─ HIGH risk → ALSO notify affected individuals without undue
delay [^10^]
                (> 500 residents or sensitive data = media notice as well)
[^8^]
```

Content of notice (Art. 33 / PCI DSS 12.10.1):

- Nature of breach, categories & approximate number of records/subjects
- Likely consequences
- Measures taken or proposed
- Contact details of DPO
- Advice on self-protection (change password, monitor statements)

Templates pre-approved by Legal reside in …/ISMS/Templates/Breach-Notice-*.docx

---

10. TIMELINE QUICK REFERENCE

TableCopy

Clock	**Action**
0 h – discovery	Triage, severity, open ticket
1 h	Contain, preserve evidence

4 h	Preliminary root-cause & impact statement
24 h	Finalise risk assessment; decide on notifications
≤ 72 h	Submit GDPR breach form to DPC (online) & PCI form to bank
≤ 60 days (PCI)	Submit Incident Report & Root Cause to QSA if applicable
≤ 60 days (HIPAA-style)	Deliver individual notices (if required)

---

11. COMMUNICATION PATHWAYS

Internal:

Reporter → Slack #security → IC → (escalate) → CEO → Board

External:

- DPC (Ireland) – breach@dataprotection.ie + web-form
- Stripe / Acquiring bank – security@stripe.com + portal
- Affected individuals – e-mail + SMS if urgent; postal if no e-mail
- Media – only via Communications Officer after legal review
- Cyber-Insurance – within 24 h (policy #IRL-CYBER-2025-001)

---

12. DOCUMENTATION & EVIDENCE

- All actions time-stamped in Jira; export PDF for regulator
- Chain-of-custody form for any hardware seized
- Decision-log signed by IC – used for post-mortem and “lessons-learned” report

---

13. POST-INCIDENT ACTIVITY

- Lessons-learned meeting ≤ 5 business days after closure
- Update policies, playbooks, monitoring rules as indicated
- Track corrective actions in Jira; verify completion before signing off
- Share anonymised summary with all staff (awareness)

---

14. METRICS & CONTINUOUS IMPROVEMENT

Quarterly dashboard reported to management:

- **incidents by severity**
- Mean-time-to-detect (MTTD) – target < 2 h
- Mean-time-to-contain (MTTC) – target < 4 h
- % incidents with evidence package complete
- % breaches notified inside 72 h – target 100 %

---

15. TRAINING & TESTING

- New-starter security induction includes “how to report”
- Annual phish + breach simulation; inject fake alert to Slack
- Table-top scenarios: ransomware, lost laptop, stolen API key

---

16. RETENTION

Incident tickets & evidence retained 3 years (PCI DSS 10.3) or longer if litigation likely.

---

17. CONTACTS QUICK LIST

TableCopy

Function	24 h reachable
IC / DPO – Michael	+353 87 000 0001

IR team e-mail	ir@paperworks.ie
External forensics	IR-Retainer@cyberlab.ie
Cyber-insurer	claims@insuretech.ie
AWS support (P)	+1 206-555-1234 (Enterprise)

---

18. DOCUMENT CONTROL

Owner: Pam Kelleher

Location: …/ISMS/POL-06-Incident-Response.pdf

Public summary: https://paperworks.ie/security

Related docs:

- Business Continuity Plan (POL-07)
- Access Control Policy (POL-04)
- Data Protection & Privacy Policy (POL-05)