Logging & Monitoring 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 every security-relevant event across PaperWorks systems is captured, stored, protected, reviewed and retained in a manner that:
- Satisfies PCI DSS v4.0 Req. 10, 12.10.5
- Supports GDPR Art. 32 “technical & organisational measures”
- Enables ISO 27001 A.12.4 (logging) & A.16.1 (monitoring) audits
- Provides evidence for incident response, forensics and legal discovery

2. SCOPE
   Applies to all assets in scope of the ISMS: production web server, database, cloud consoles, VPN, endpoints, POS integrations, SaaS (Stripe, G-Suite, Shopify) and any system that stores, processes or transmits personal or card-holder data.
3. OBJECTIVES
- Detect unauthorised access within minutes
- Reconstruct transaction history for at least 12 months
- Guarantee log integrity (tamper-evident & WORM)
- Automate alerting for high-risk events
- Minimise storage cost while meeting retention mandates

4. ROLES & RESPONSIBILITIES
   Role (Name) | Responsibilities
   Incident Response Lead (Pam) | Policy owner, log-review scheduler, SIEM admin
   Security Analyst (rotating) | Daily alert triage, weekly summary
   Line Managers | Respond to user-behaviour anomalies
   Cloud Ops | Ensure agents deployed, clocks synced, disk space
   HR | Provide leaver lists for account-review logs
   CEO / DPO | Approve exceptions, review quarterly metrics

5. LOG SOURCES & MINIMUM DATA SET
   Source | Event types | Local buffer | Forward to SIEM
   AWS ALB / WAF | requestMethod, URI, userAgent, sourceIP, status, bytes, TLS-cipher, block-action | 30 days | Yes
   Nginx on EC2 | access & error, response time | 7 days | Yes
   MariaDB | connect, query, failed-login, grant, slow-query (>2 s) | 30 days | Yes
   Linux OS | auth.log, sudo, cron, file-integrity (AIDE) | 90 days | Yes
   AWS CloudTrail | console & API calls, root usage, MFA | 90 days | Yes
   Stripe webhooks | payment_intents, refunds, dispute.created | 1 year | Yes
   VPN (WireGuard) | peer connect, bytes, duration | 90 days | Yes
   Google Workspace | login, admin, Drive share, 2-step verify | 1 year | Yes
   Endpoint (Win/Mac) | process exec, USB mount, firewall block | 30 days | Yes
   Physical CCTV | entry to office | 30 days | No (separate DVR)

Minimum content per log:

- Timestamp (UTC, NTP-synced)
- Severity / priority
- User identity (local or SSO)
- Source IP & port
- Object / resource accessed
- Outcome (success / failure)
- Optional: bytes transferred, SQL statement hash, file hash

6. CLOCK SYNCHRONISATION
   All systems use pool.ntp.org; max drift 1 s. CloudWatch “TimeSyncCheck” metric alarms if > 5 s.
7. SIEM & LOG AGGREGATION
   Tool: Graylog Enterprise (open-core) on dedicated t3.medium instance;

- Ingestion via Beats / Syslog-TLS on TCP 6514 (TLS 1.3, mutual auth)
- Parsing rules normalise to GIM (Graylog Schema) for dashboards
- Hot storage 30 days, warm 11 months on Amazon S3 Glacier Instant (WORM) – total 1 year online

8. PROTECTION & INTEGRITY

- Write-once-read-many (WORM) enforced by S3 Object Lock (compliance mode, 1 year)
- SHA-256 checksum calculated at ingestion; mismatch triggers alert
- Logs stored separately from production servers (different AWS account)
- Access controlled by IAM least-privilege group “LogAdmins”; MFA mandatory

- No one may alter or delete logs before retention expires; only “archive & purge” after 1 year

9. RETENTION SCHEDULE
   Type | Online SIEM | WORM archive | Purge
   Security event | 1 year | 1 year | After 2 years
   Transaction audit | 1 year | 6 years (ROI Revenue) | After 7 years
   System debug | 30 days | N/A | After 30 days
   CCTV | 30 days DVR | N/A | After 30 days
10. REVIEW REQUIREMENTS

- Daily (automated): critical alerts (see § 11)
- Weekly (manual): Security Analyst reviews dashboard anomalies, failed logins, privilege escalations; summary posted to Slack #security
- Monthly: Pam exports exception report for management meeting (MTTD, #alerts, false-positive rate)
- Quarterly: spot check 10 % of archived logs for integrity; file SHA-256 must match
- Annually: full policy & tool effectiveness review; feed into ISMS management review

11. ALERTING THRESHOLDS (examples)
    Alert name | Count window | Action
    Root login on prod DB | 1 | Page IC immediately

20 failed logins from single IP | 10 min | Block IP, ticket

WAF block rate > 500 / 5 min | 5 min | Ticket

New API key created | 1 | Slack #security

Log forwarding stops > 5 min | 5 min | Page Ops

Geo-impossible travel (same user) | 30 min | Ticket + e-mail user

Card-holder data regex in app log | 1 | Page + containment

AIDE checksum change on /etc | 1 | Ticket

Escalation: Slack → PagerDuty → phone call if not acknowledged in 15 min.

12. ENDPOINT & APPLICATION LOGGING

- Centralised osquery schedule captures USB mount, listening ports, browser plugin changes
- Web-app writes structured JSON (trace-id) to stdout; captured by Vector sidecar → SIEM
- No full PAN or CVV ever written to log (PCI DSS 3.5.4) – filtering rule drops 15+ digit numbers

13. THIRD-PARTY / SAAS LOGS

- Google, Stripe, Shopify logs retained in vendor console for vendor-native period; we additionally export daily JSON dump to S3 WORM for 1 year
- Vendor logs are accepted only if they meet PCI 10.2/10.3 content requirements

14. EXCEPTIONS

Any deviation (e.g., shorter retention for debug nodes) must be:

15. Risk-assessed and documented
16. Approved by CEO & DPO
17. Reviewed at next policy cycle
18. TRAINING & AWARENESS

- Analysts complete “Graylog Power User” & “SIEM rule writing” courses
- Annual phishing simulation includes “did you report the alert?” metric

16. METRICS REPORTED TO MANAGEMENT

- Mean-time-to-detect (MTTD) – target < 2 h
- Mean-time-to-respond (MTTR) – target < 4 h
- % high-severity alerts triaged within SLA (24 h) – target 100 %
- % archived logs passing integrity check – target 100 %
- Storage cost vs budget – variance < 10 %

17. COMPLIANCE MAPPING

ISO 27001 A.12.4.1 / A.12.4.3 / A.16.1.1
PCI DSS 10.2, 10.3, 10.4, 10.5, 10.6, 10.7, 12.10.5
GDPR Art. 32(2) – ability to recreate processing sequence

18. DOCUMENT CONTROL

Owner: Pam Kelleher
Location: …/ISMS/POL-08-Logging-Monitoring.pdf
Related docs:

- Access Control Policy (POL-04)
- Incident Response Policy (POL-06)
- Backup Policy (POL-09)