Incident Response Tabletop — Ransomware Scenario

Documents a facilitated tabletop exercise, participants, decisions, gaps identified and follow-up actions.

SAMPLE — anonymised demo data. Real exports carry your organisation branding, control mappings and signed timestamps.

Evidence ID	EV-2026-IR-02
Owner	J. Patel, Head of Security
Generated	2026-06-30 09:14 UTC
Framework(s)	ISO 27001, SOC 2, PCI DSS
Control(s)	A.5.24–A.5.27 · CC7.4 · Req 12.10
Next review	2027-04-30

Scenario

Ransomware detected on a developer laptop with cached production credentials. Objective: exercise detection→containment→eradication→recovery→notification decisions under time pressure.

Participants

Head of Security (IC), SRE on-call, Legal, CS Lead, CEO (observer), external DFIR retainer (dial-in).

Outcome

Phase	Target	Observed	Notes
Detection→Containment	≤ 30m	18m	EDR isolated device, creds rotated
Regulator clock started	≤ 60m	42m	DPO paged, timer started
Customer comms drafted	≤ 4h	2h 10m	Template + legal review path
Post-incident review	≤ 5 business days	Booked	Scheduled 2026-06-08

Gaps & actions

Two gaps: (1) DFIR retainer contact list stale — updated same day; (2) internal comms bridge auto-record was off — enabled and documented in runbook. Both actions closed and evidenced.