**ADD-02 — Incident Response & Breach Notification Runbook**

**Status:** New

**Intent**  
React fast, lawfully, and consistently to security incidents; notify customers & authorities within required timelines.

**Actors**  
IR Lead • SOC • Legal • Comms • Engineering • Audit Vault

**Preconditions**

* On-call rotations and contact trees exist.
* Log retention + evidence capture enabled.

**Flow**

1. **Classify Incident:** severity & data impact (PII, secrets, tokens).
2. **Containment:** disable affected creds/paths; enable kill-switches if needed.
3. **Forensics:** snapshot logs, DBs, object versions; compute incident hash list.
4. **Assessment:** did personal data/sanctions data leak? which regions?
5. **Comms:** templates for tenant & regulator notices; timelines per jurisdiction (e.g., 72h for GDPR).
6. **Remediation:** patch, rotate keys, extra monitoring.
7. **Post-mortem:** 5 whys; action items with owners & deadlines; publish tenant-visible summary (no secrets).
8. **Drill:** tabletop twice/year; store drill evidence.

**Edge Cases**

* Multi-region breach → separate regulator notifications with region facts.
* Third-party breach → coordinate with processor; include their attestations.

**Done when**

* MTTR & notification timelines met in drills; post-mortems tracked to closure.
* Rotations + playbooks accessible; last drill report in Audit Vault.

**Deliverables**  
Runbook, comms templates, drill reports, corrective action tracker.