

The First 24 Hours, on one page

The breach response checklist, condensed for print. Full version with the reasoning:
vendorquals.com/blog/breach-response-checklist

HOURL 0–1: CONTAIN, PRESERVE, CALL

- ✓ Isolate affected systems at the network level. Do NOT power off encrypted machines; volatile data is evidence.
- ✓ Do NOT reimage, restore, or clean anything before forensics. That evidence serves the claim, the regulator, and the case.
- ✓ Log the discovery time to the minute. Every clock keys off it.
- ✓ Start the incident log: every action, decision, and time goes in it.
- ✓ CALL IN ORDER: 1. Your carrier's breach hotline (panel rules and reimbursement depend on it). 2. Counsel (response runs under privilege). 3. Your retainer firm or responder selection.

HOURS 1–4: SCOPE AND COMMAND

- ✓ Name the incident commander: one person with authority to spend and decide.
- ✓ Establish out-of-band comms if email may be compromised; one authorized voice.
- ✓ Begin scoping: systems, data types, credentials, third parties.

HOURS 4–24: THE CLOCKS AND THE RESPONSE

- ✓ Start the notification matrix (see the clocks sheet): GDPR 72h, HIPAA 60d, state laws, sector regulators.
- ✓ Check the carrier panel before engaging any off-panel firm; get pre-approval in writing.
- ✓ Ransomware: no payment decision in hour six; establish scope, backups, and sanctions screening first.
- ✓ Brief the board: what is known, what is not yet known, what happens next. Facts with timestamps, no promises.

NEVER, AT ANY HOUR

- ✓ Never reimage or delete attacker artifacts before forensics.
- ✓ Never email the attacker from your own mailbox.
- ✓ Never promise a scope you have not confirmed.
- ✓ Never let two people speak for the organization.

Who to call when inside an incident: vendorquals.com/blog/breached-right-now-choosing-a-responder. The plan this sheet belongs in:
vendorquals.com/incident-response-plan-template.docx

Free, no signup, from vendorquals.com, the evidence-graded incident response firm directory. Not legal advice; verify current rules with counsel before relying on them. Guides behind this sheet: vendorquals.com/blog/state-breach-notification-laws,
vendorquals.com/blog/financial-services-breach-notification, vendorquals.com/tools/breach-cost-calculator