Best-practice incident response playbook

First-step operational checklist for the first 24 to 72 hours after discovering a suspected incident. These are best practices, not statutory deadlines.

Examples

- Preserve logs and evidence before cleanup or rebuilding.
- Open an incident ticket, assign an owner, and start a decision log.
- Capture an incident timeline with containment and restoration milestones.
- Notify counsel, cyber insurance, and critical response partners early.
- Confirm state, regulator, FTC, IRS, and contract-specific notification triggers before sending notices.

Use counsel and jurisdiction-specific rules to make actual notice decisions.