Safe Action Playbook — Example

Scenario: No■patch critical vulnerability in Lab Controller X

IMPACT: RED — Direct Care Threat

Summary

Vulnerability may allow remote calibration changes; no vendor patch available. Mitigate to protect diagnostic accuracy.

Pre■checks

- Confirm device is actively used in clinical/production workflow.
- Verify affected model/firmware from vendor bulletin; note serial/asset ID.

Do NOT

- Do not power■cycle mid■run or interrupt active diagnostics/production.
- Do not pull device from service without approved fallback.

Actions — Do This Today

- Isolate: restrict device network access to required subnets/services only.
- Credentials: rotate local creds/MFA where applicable; disable default accounts.
- Monitoring: enable verbose logs; start a manual log for abnormal temps/restarts.
- Compensating controls: apply vendor■recommended mitigations; increase QA spot■checks.
- Stakeholders: notify clinical/production leads of temporary risk and mitigations.

Escalation — When to Call Tier■2

- Any abnormal temperature/reading drift or device instability.
- Evidence of active exploitation on your network.
- No viable mitigations in regulated use (clinical/GMP/food).

Posture & Recovery

- Schedule patch window immediately when available; verify calibration after patch.
- Keep device in segmented posture until two clean QA cycles.

Audit Notes (fill in)

Record: timestamp, user, asset ID, mitigations applied, anomalies observed, contacts notified.