

Incident Response Plan

Phases: Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned.

Roles: Incident Commander, Comms, Forensics, Legal/Privacy, Business Owner.

Runbook: Triage -> Isolate -> Eradicate -> Recover -> RCA.