



SAMPLE OPERATING PLAN

Incident Response Plan + Tabletop Record

A concise, practical sample for defining severity, escalation, first-hour actions, communications, evidence preservation, and lessons learned.

Incident Response Plan + Tabletop Record

A concise operating artifact for recognizing, escalating, managing, documenting, and learning from security incidents.

Purpose

Provide a clear, proportionate response path for security events. This sample demonstrates operating guidance; it is not emergency legal, forensic, or incident-response retainership advice.

Severity levels

Level	Description	Examples	Response expectation
SEV 1 — Critical	Confirmed or likely event with material business, customer, legal, or operational impact.	Ransomware, confirmed customer-data exposure, privileged account compromise.	Escalate immediately; activate incident lead and executive authority.
SEV 2 — High	Significant suspected event with limited confirmed impact or material potential.	Suspicious inbox rule, malware alert, exposed credential, critical vendor notification.	Escalate same business day; investigate, contain, document.
SEV 3 — Moderate	Suspicious event requiring review; impact not confirmed.	Reported phishing, lost device with controls, unusual login.	Triage promptly; document disposition and follow-up.
SEV 4 — Low	Routine security request or non-material event.	Training question, benign scan, policy clarification.	Route through normal security operations.

Response roles and authority

Role	Primary responsibility	Decision authority
Incident Lead	Coordinates assessment, timeline, containment work, evidence log, and follow-up.	Recommends severity and containment actions.
Executive Sponsor	Ensures business continuity, resources, and executive decisions.	Approves material business interruption and risk acceptance.
IT / Provider	Performs technical containment, recovery, and system validation.	Executes approved changes within assigned scope.
Legal / Privacy advisor	Advises on notification, privilege, contracts, and regulatory implications.	Advisory; legal determinations remain with counsel.
Communications owner	Coordinates employee, customer, partner, and media communications.	Publishes approved messages only.

First-hour response actions

The first hour focuses on safety, containment, decision quality, and preserving enough information to understand what happened. Avoid broad changes that destroy evidence or create unnecessary business disruption without an approved decision.

Time	Action	Owner	Evidence / output
0-10 min	Record report, preserve original details, assign incident lead, and set provisional severity.	Reporter / Incident Lead	Incident record; initial timeline
10-20 min	Validate facts; identify affected accounts, systems, data, and business process.	Incident Lead + IT	Scope notes; affected asset list
20-35 min	Contain proportionately: revoke sessions, reset credentials, isolate device, disable rule, or restrict access.	IT / Provider	Containment actions and timestamps
35-50 min	Notify executive sponsor and counsel/privacy contact for SEV 1-2 events.	Incident Lead	Decision log; contact record
50-60 min	Set next update time, preserve evidence, assign investigation and recovery work.	Incident Lead	Action register; evidence inventory

Communication and evidence rules

Topic	Operating rule
Internal updates	Share facts, impact, action owners, and next-update time. Avoid speculation and unapproved external statements.
External communication	Customer, regulator, insurer, and media communication requires executive and legal approval where applicable.
Evidence preservation	Preserve relevant messages, logs, screenshots, timestamps, affected-account details, configuration snapshots, and decision records.
Insurance / specialist support	Contact cyber-insurance carrier, legal counsel, digital forensics, or managed-security partner according to applicable contracts and incident severity.
Recovery and lessons learned	Validate restoration, document remaining risk, record corrective actions, and conduct a post-incident review.

Escalation trigger

Any suspected exposure of customer data, compromise of privileged access, ransomware indicator, or material disruption is treated at least as SEV 2 until the Incident Lead and Executive Sponsor agree otherwise.

Tabletop exercise record

Scenario: Business email compromise — a finance employee reports a message appearing to come from the CEO requesting an urgent update to bank-account instructions. The employee clicked a link but did not enter credentials.

Scenario	Exercise date	Participants	Exercise result
BEC	Oct 17	6	Improvement
Urgent executive request	Illustrative record	Leadership + IT	Actions assigned

Discussion timeline

Prompt	Expected decision / action	Observed result
How is the event reported?	Employee forwards message through approved reporting path; Incident Lead opens record.	Reporting process was understood.
What is contained first?	Validate click, revoke active sessions if needed, inspect mailbox rules, reset credentials only if compromise evidence exists.	Team identified appropriate steps; mailbox-rule check added.
Who decides whether to notify leadership?	Incident Lead escalates as SEV 2 until scope is confirmed; Executive Sponsor receives status.	Escalation threshold accepted.
What evidence is retained?	Original message, URL, timestamps, account/audit logs, actions taken, and decision log.	Evidence list requires template.
How is learning shared?	Targeted refresher on urgent financial requests and out-of-band verification.	Training action approved.

Corrective actions

Action	Owner	Due	Status
Add finance-request verification guidance to awareness training	Security Owner	Oct 31	Open
Create incident evidence checklist in Unboredly	Operations Lead	Nov 07	Planned
Confirm cyber-insurance notification contact and process	Executive Sponsor	Nov 15	Open
Schedule second tabletop: ransomware disruption	Incident Lead	Dec 10	Planned

Exercise conclusion The exercise validated the basic escalation path while identifying gaps in evidence capture and finance-request verification. The corrective actions above should be reviewed at the next security-program meeting.