BRISKDATA ENGINEERING TEMPLATE | DOC ID: BD-SEC-IR-002 | ADAPTABLE TEMPLATE

Incident Response Runbook Template

Severity Policy, Responder Roles, Evidence Preservation, Containment, and Communications

EVIDENCE PRESERVATION RULE

Separate availability outages from suspected security compromises immediately. During a suspected intrusion, do not reboot, wipe, or delete affected servers before isolating network access and capturing disk snapshots, memory/process state, and authentication logs.

1. Runbook Ownership and Escalation Contacts

Role / Channel	Primary Contact / Location	Alternate / Out-of-Band Path
Covered Systems & Scope	[Production applications, cloud accounts, corporate identity]	[Exclusions / partner-managed systems]
Incident Commander (IC)	[On-Call Rotation / Pager Link]	[Backup IC / Phone]
Technical & Security Leads	[Platform Lead] | [Security Lead]	[External IR Retainer / Hotline]
Communications & Legal	[Comms Owner] | [Legal Counsel / Breach Coach]	[Out-of-band bridge if primary chat/mail impaired]

2. Example Severity Policy and Crosswalk (Adapt to Team Agreements)

Teams using S0-S3 or SEV-1 to SEV-4 labels can map them directly using the crosswalk below. Response and update intervals are adaptable internal targets rather than external SLAs unless incorporated into a contract.

Severity Label	Operational or Security Trigger Definition	Target Ack	Status Update Cadence	Core Responders
SEV-1 (S0)	Full service outage, active credential/ransomware intrusion, or confirmed exposure of regulated data.	5 - 15 min	Every 15 - 20 min	IC, Tech Lead, Sec Lead, Comms, Exec/Legal
SEV-2 (S1)	Major workflow degradation (e.g., checkout/sign-in impaired) or single-host security containment.	15 min	Every 30 min	IC, Tech Lead, Sec Lead, Comms, Scribe
SEV-3 (S2)	Partial feature impact with workaround or suspicious security alert under investigation.	30 - 60 min	Every 2 hours	On-Call Engineer + Peer / Sec Analyst
SEV-4 (S3)	Minor internal defect, non-urgent bug, or informational telemetry anomaly.	Next bus. day	Async in ticket	Assigned Service Owner

3. Responder Roles and Responsibilities

- **Incident Commander (IC):** Coordinates responders, owns decision gates, and approves external updates. Avoids editing code or running terminal commands personally so coordination never stalls.
- **Technical / Security Lead:** Directs operational triage, rollback execution, network quarantine, credential revocation, and forensic snapshot capture.
- **Scribe:** Records a UTC timestamped log of observed symptoms, hypotheses tested, commands executed, and state changes.

- **Communications Lead:** Publishes customer status updates, internal executive summaries, and legal/compliance hold notices on the agreed cadence.

4. First-15-Minutes Triage and Containment Tracks

Track A - Availability / Deployment Outage: Confirm blast radius, check deployments/config edits/DNS changes from the past 2 hours, and execute the service Backout Plan if correlated.

Track B - Suspected Security Compromise: Place affected hosts into a quarantine security group/VLAN without powering off, snapshot storage volumes, revoke active user/service tokens, audit mailbox forwarding/OAuth grants, and engage Legal Counsel before altering forensic artifacts.

ILLUSTRATIVE CONTAINMENT & SNAPSHOT COMMANDS (REPLACE PLACEHOLDERS FOR YOUR CLOUD / IDP)

```
# Quarantine cloud instance network access without terminating volatile memory or disks
aws ec2 modify-instance-attribute --instance-id <INSTANCE_ID> --groups <QUARANTINE_SG_ID>

# Capture timestamped forensic disk snapshot and deactivate compromised access key
aws ec2 create-snapshot --volume-id <VOLUME_ID> --description "IR-PRESERVE-$(date -u +
%Y%m%dT%H%M%SZ)"
aws iam update-access-key --user-name <IAM_USER> --access-key-id <ACCESS_KEY_ID> --status Inactive
```

5. Legal Notification Review & Closure Checklist

Confirm exact statutory and contractual reporting clocks with Legal Counsel and cyber-insurance counsel (for example: customer MSA security addenda, payment acquirer notices, HIPAA/GLBA/GDPR/state breach statutes, SEC materiality rules, or DoD DFARS 252.204-7012 where applicable).

- [ ] **Service & Security Stabilized:** Error rates, latency, and security telemetry verified clean for at least 30 consecutive minutes.
- [ ] **Secrets & Sessions Rotated:** Affected passwords, refresh tokens, API keys, OAuth grants, and webhook secrets rotated.
- [ ] **Post-Incident Review Scheduled:** UTC timeline preserved and blameless review booked within [2 business days] with owned remediation tickets.

Template Reuse Note: You may copy and adapt this template for internal operations within your organization. Replace bracketed placeholders and remove example entries before adoption. briskData branding and third-party trademarks remain the property of their respective owners.