

Incident Response Plan

Purpose

Your Organization must be able to detect, triage, contain, eradicate, and recover from security incidents in a consistent, timely, and auditable manner. This plan defines the process, roles, and communication requirements used by Your Organization when responding to a suspected or confirmed information security incident.

Scope

This plan applies to all Your Organization information systems, data, workforce members, and third parties who handle Your Organization data. It covers incidents affecting confidentiality, integrity, or availability of Your Organization systems or data — including malware, unauthorized access, account compromise, data exfiltration, denial of service, insider misuse, and vendor-reported incidents.

Definitions

- **Event.** An observable occurrence in a system or network.
- **Incident.** An event (or series of events) that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information it processes.
- **Breach.** An incident resulting in confirmed disclosure of protected data to an unauthorized party.

Severity matrix

Severity	Definition	Target triage	Exec notification
SEV-1	Confirmed breach of regulated or highly confidential data; production outage affecting customers	Immediate	Within 1 hour
SEV-2	Confirmed unauthorized access without confirmed data loss; significant internal outage	Within 1 hour	Within 4 hours
SEV-3	Contained policy violation; minor malware infection successfully quarantined	Within 4 hours	Next business day
SEV-4	Suspicious event requiring investigation; no confirmed impact	Within 1 business day	Weekly status

Roles

- **Incident Commander (IC).** Owns the incident end to end, makes the call on classification, escalation, and external communications. Designated on rotation from the security team.

- **Scribe.** Maintains the incident timeline, captures decisions, evidence, and actions taken.
- **Technical Lead.** Drives containment, eradication, and recovery actions with engineering.
- **Communications Lead.** Owns internal and external communications; coordinates with Legal and PR as needed.
- **Legal Counsel.** Advises on regulatory notification obligations and evidence handling.
- **Executive Sponsor.** CISO or designee; owns executive-level decisions and resource allocation.

Lifecycle

1. Preparation

Maintain asset inventory, tested backups, logging pipelines, on-call rotations, runbooks, and annual tabletop exercises.

2. Detection and analysis

Triage alerts from monitoring, user reports, and third-party notifications. The on-call analyst creates an incident record, assigns provisional severity, and pages the IC if SEV-1 or SEV-2.

3. Containment

Short-term: isolate affected accounts, hosts, or network segments to stop active harm. Long-term: apply configuration and architectural changes to prevent recurrence during the investigation.

4. Eradication

Remove the threat: kill malicious processes, revoke credentials, apply patches, remove unauthorized accounts, rotate keys and secrets, rebuild compromised systems from trusted media.

5. Recovery

Restore affected systems from known-good backups or rebuilt images. Validate integrity, confirm logging is intact, and monitor for signs of re-compromise before closing.

6. Post-incident review

Within 10 business days of closure, conduct a blameless post-incident review. Capture root cause, lessons learned, and remediation actions. Publish a written report to the CISO and the executive sponsor.

Notification obligations

Your Organization assesses every incident for regulatory, contractual, and customer notification obligations (GDPR, HIPAA, CCPA, state breach-notification laws, customer contracts). Legal Counsel owns the notification-decision flow and must be consulted before any external disclosure.

Evidence handling

Evidence must be collected following chain-of-custody principles. Logs, disk images, memory captures, and email exports must be hashed, time-stamped, stored in a tamper-evident location, and retained for at least three

years or as required by law or contract.

Testing

This plan is tested at least annually via a tabletop exercise driven by the CISO's office. Exercise findings feed the preparation activities above.

Review cadence

This plan is reviewed annually by the CISO, the Incident Commander pool, and Legal Counsel, or sooner following any SEV-1 incident or material change to Your Organization's technology footprint.

Effective date: [the date this policy takes effect]