

Incident Response Plan

Use this plan to prepare and coordinate incident handling, preserve decision records and guide scenario-specific response. Complete actual authority, evidence controls and notification rules before use. Repeat the playbook module only for scenarios covered by your approved response capability.

Complete bracketed fields with approved information. Duplicate modules and rows as needed; record the reason for any section marked not applicable.

Document [ID and revision] **Owner** [Role] **Scope** [Organization, site or product]

Effective date [Date] **Approval** [Controlled record] **Next review** [Date or trigger]

Plan foundation

Foundation	Approved response arrangement
Mission objectives and scope	[Services, assets, data, locations and exclusions]
Authority and lifecycle	[Management authorization, phase names and model adopted]
Related plans	[Continuity, disaster recovery and crisis communications interfaces]

Incident definitions and classification

Category or severity	Exact criteria and declaration threshold	Decision and clock basis
[Event, alert or incident definition]	[Approved distinction and criteria]	[Authority and record]
[Priority or severity label]	[Impact, scope and escalation threshold]	[Clock start, target if adopted and source]

Roles and responsibilities

Role or team	Responsibility and high impact decisions	Handoff and contact reference
[Incident lead and handler]	[Declaration, isolation or shutdown authority]	[Verified directory and succession]
[Legal, communications or business role]	[Notification, disclosure or service decision]	[Approval and coordination route]
[Provider or third party]	[Contracted boundary and required cooperation]	[Agreement and acknowledgement]

Preparation

Readiness area	Required capability or check	Evidence and outstanding gap
[Tools, logs, access or secure communications]	[Coverage, availability and approved readiness criterion]	[Test record and owner]
[Training or exercise]	[Scenario, roles and objective]	[Result and improvement]

Detection and analysis

Incident intake and triage record

Field	Verified facts and decision
Incident ID discovery and report	[Time with zone, source, reporter role and channel]
Affected assets and impact	[Scope, business effect and confidence level]
Analysis and classification	[Indicators, evidence references, severity and rationale]
Declaration and escalation	[Authority, decision time and notified roles]
Investigation plan	[Next questions, assigned tasks and evidence controls]

Evidence and decision log

Time and item	Action or decision with rationale	Actor authorization and custody
[Time zone; evidence or decision ID]	[Verified observation, action, source and rationale]	[Role, approval, transfer and secure record location]
[Entry]	[Action and result]	[Custody and integrity reference]

Containment eradication and recovery

Phase	Approved task and entry condition	Verification and authorization
Containment	[Scope, evidence preserved first and controlled action]	[Impact assessment, authority and result]
Eradication	[Root cause and approved removal action]	[Checks and remaining exposure]
Recovery	[Restore sequence and acceptance criteria]	[Data/service validation and return authority]

Repeatable incident scenario playbook

Playbook setup		Scenario specific information
Scenario scope and triggers		[Indicators, alerts and conditions that activate this playbook]
Severity and escalation		[Link to classification; exact trigger and authority]
Resources and precautions		[Tools, access and approved warnings before risky actions]
Phase and step	Action and decision point	Evidence result and authority
Detection and analysis 1	[Verify indicator and scope; if condition then action]	[Evidence and classification]
Containment 2	[Preserve required evidence, then approved containment]	[Authorization, impact and result]
Eradication 3	[Address verified cause using controlled procedure]	[Result and residual issue]
Recovery 4	[Restore and validate within approved boundary]	[Acceptance and service-owner decision]
Post incident 5	[Complete required review and closure]	[Closure criterion and record]

Communication and reporting

Recipient and trigger	Approved message channel and authority	Timeframe and evidence
[Internal role or external party]	[Verified facts, required content, secure channel and approver]	[Exact adopted requirement; clock start and sent/received record]
[Stakeholder update]	[Impact, action, uncertainty and next update]	[Approved cadence and distribution]

Post incident activity and plan maintenance

Review element	Evidence conclusion and action
Timeline and response effectiveness	[What occurred, decisions, delays and observed outcomes]
Root cause and lessons	[Established causes, contributing conditions and gaps]
Corrective actions	[Owner, due date, evidence and effectiveness check]
Records metrics and retention	[Approved measures, calculation, storage and retention rule]
Plan update and exercise	[Change, approver, communication and retest]

Quick reference

First response card

Need	Approved immediate instruction
Recognize and report	[Indicator and verified first contact route]
Immediate do and do not actions	[Only actions and prohibitions adopted for this environment]
Evidence and service protection	[Approved preservation and safety instructions]
Full response material	[Offline-accessible plan, classification and playbook links]

Escalation directory

Condition	Destination and fallback	Current owner and acknowledgement
[Approved trigger]	[Role/team and verified directory reference]	[Ownership, response requirement and record]

Release readiness

- ☐ Authorities, evidence safeguards, communications and scenario actions are verified.
- ☐ No secrets appear in the plan; secure access references have been tested.

Review role	Decision and date	Open actions and approval reference
[Response authority]	[Approved or returned]	[Controlled record and next review]