

Incident Response Plan Template

A free, fill-in-the-blank template covering roles and backups, severity tiers, a communication tree, phase-by-phase response steps, documentation, and SOC 2 / ISO 27001 / HIPAA / GDPR alignment.

Company: _____

Effective date: _____

Plan owner: _____

Review cycle: Annually, after any major system or team change, and after every real incident or tabletop exercise

HOW TO USE THIS TEMPLATE

Replace every bracketed placeholder with your organization's specifics, complete the blank tables, and route the finished plan through your normal approval process. Sample times and thresholds are illustrative starting points, not benchmarks. This template is the operational runbook a responder opens mid-incident; the governance document (ownership, scope, review cadence) is your incident management policy. This template is a starting point, not legal advice. See ComplyJet's [Incident Response Plan Template guide](#) for the reasoning behind each section.

1. Purpose and Scope

This plan defines how [Company Name] detects, contains, eradicates, and recovers from security incidents, and how the team communicates while doing so. It applies to all employees, contractors, and in-scope systems listed in [system inventory or asset register]. It is an operational runbook. Why the program exists, who owns it, and how often it is reviewed are set out in the [Incident Management Policy]. Restoring systems after an outage or disaster is covered in the [Disaster Recovery Plan].

2. Incident Response Team: Roles and Backups

Every role has a named backup. A plan with one name per role is a single point of failure. Confirm contact details quarterly and store this list somewhere reachable when your primary systems are not.

Role	Responsibility	Primary	Backup	Phone / pager
Incident commander	Owens decisions during the incident, assigns severity, coordinates the response	[Name]	[Name]	[]
Technical lead	Drives containment, eradication, and recovery on the systems side	[Name]	[Name]	[]
Communications lead	Owens internal updates and all external notification, so technical responders are not drafting customer emails	[Name]	[Name]	[]
Scribe / logger	Keeps the incident log (Section 8) as events happen	[Name]	[Name]	[]
Legal / privacy contact	Advises on regulator and customer notification duties	[Name]	[Name]	[]
Executive sponsor	Receives escalations; approves major business decisions	[Name]	[Name]	[]
[Add role]				

Reporting channel (how anyone raises a suspected incident): [e.g. #security-incidents Slack channel, security@company.com, on-call phone]. Contact list location (stored outside the environments being defended): [Location].

3. Severity Classification

The incident commander assigns an initial severity within [15 minutes] of a report and may revise it as more information arrives. Tie every tier to concrete triggers, not a "use your judgment" scale.

Tier	Trigger (sample)	Response target (sample)	Your triggers / targets
Critical	Confirmed unauthorized access to customer data, or a full production outage	Commander engaged immediately; all-hands response	[]
High	Suspected unauthorized access, or a partial service degradation	Commander and technical lead within 15 minutes	[]
Medium	Internal-only anomaly with no confirmed customer or data impact	Triage within [4 hours]	[]
Low	Policy violation with no active security risk	Triage within [1 business day]	[]

4. Communication Tree

Who notifies whom, in what order, within what timeframe. The sample for a Critical incident is shown; complete the table below it for each tier. Cover customers and regulators, not just internal escalation, and name an owner for each. Log every notification and timestamp as it happens.

1. Reporting party notifies the **Incident commander** immediately

within 15 minutes

2. Incident commander notifies the **Technical lead** and the **Communications lead**

then the **Communications lead** triggers, each on its own timer

Internal leadership
within 30 minutes

Affected customers
within [] hours, as required

Regulators / auditors
per framework deadline (see Section 9)

Tier	Internal escalation (who, how fast)	Customers	Regulators / auditors	Legal / leadership
Critical	[]	[]	[]	[]
High	[]	[]	[]	[]
Medium	[]	[]	[]	[]
Low	[]	[]	[]	[]

5. Phase-by-Phase Response

The phases follow the structure NIST's incident response guidance (SP 800-61) is organized around. Adapt the sample language to your own systems and tooling.

1 Preparation

Named roles and backups are recorded in Section 2. Logging covers [systems, cloud accounts, identity provider]. Responders have access to [tools, runbooks, contact list]. The plan is read by all team members on hire and [annually]. A tabletop exercise is run [annually].

Owner: _____ **Last completed:** _____

2 Detection and Analysis

Anyone who suspects an incident reports it via [reporting channel] immediately. The incident commander confirms whether the event is real, assigns a severity per Section 3, opens an incident record, and assigns a scribe. Initial analysis identifies affected systems, data, and the likely entry point, and preserves relevant logs before they roll over.

Owner: _____ **Target:** severity assigned within [15 minutes]

3 Containment

The technical lead stops the incident from spreading without destroying evidence: isolate affected hosts, revoke or rotate exposed credentials, block malicious IPs, and disable compromised accounts. Snapshot affected systems before changes where possible. Record every action in the incident log.

Owner: _____ **Decision needed from commander before:**

4 Eradication

Remove the actual cause, not just the symptom: delete malicious artifacts, patch the vulnerable service, fix the misconfigured permission, and reset all credentials that may have been exposed. Confirm the root cause is understood before moving to recovery.

Owner: _____ **Root cause:** _____

5 Recovery

Restore affected systems from known-good sources, return them to production in a controlled order, and monitor closely for [days/weeks] to confirm the threat is gone, not just quiet. The incident commander formally closes the incident once recovery is verified.

Owner: _____ **Monitoring period:** _____

6 Post-Incident Review

Within [5 business days] of closure, hold a blameless review covering timeline, what worked, what did not, and the root cause. Record action items with owners and due dates, and update this plan accordingly. This is the phase most plans skip and the one auditors probe on: keep the written review as evidence.

Owner: _____ **Review held on:** _____

6. Detection and Reporting Checklist

- ☐ Every employee knows the reporting channel and that reporting is expected, not optional.
- ☐ Reports are acknowledged within [15 minutes], including outside business hours.
- ☐ Alerts from [monitoring / SIEM / cloud] route to the on-call responder.
- ☐ Third-party and customer reports are routed to the same channel.

7. Escalation Triggers

Escalate to legal and executive leadership immediately when any of the following is true: customer or personal data is confirmed or suspected exposed; a regulator or law enforcement contact is needed; ransom or extortion is involved; the incident is expected to exceed [4 hours]; [add your own].

8. Incident Log Template

Log as you go, not after. The timeline, the actions taken, the decisions made, and who made them are what an auditor asks to see, not a recap reconstructed from memory.

Incident ID		Severity	
Reported by		Detected at	
Commander		Closed at	

[illegible]

9. External Notification and Framework Map

Each framework sets incident response expectations in a different place. Map your plan once and rehearse it the same way regardless of which auditor is asking.

Framework	Where it lives	What it expects	Your plan section
SOC 2	Trust Services Criteria CC7.3 and CC7.4	A documented process for identifying, responding to, and communicating about security incidents, plus evidence it is actually followed	Sections 2 to 5, 8
ISO 27001	Annex A controls 5.24 to 5.28 (Information security incident management)	Incident planning and preparation, assessment of events, response, learning from incidents, and evidence collection, as five distinct auditable controls	Sections 5, 8, 10
HIPAA	Security Rule, 45 CFR 164.308(a)(6), Security Incident Procedures	Policies and procedures to address security incidents, including a response and reporting process; the regulation does not prescribe specific plan content	Sections 4, 5
GDPR	Articles 33 and 34	Notify the supervisory authority within 72 hours of becoming aware of a personal data breach; notify affected individuals directly when the risk to them is high	Sections 4, 7

Notification deadlines that apply to us (customer contracts, state breach laws, cyber-insurance carrier):

Confirm exact current wording against the live AICPA TSC, ISO/IEC 27001:2022, HIPAA, and GDPR text. This is a starting reference, not a substitute for reading each framework's current requirements.

10. Testing and Plan Maintenance

1. **Schedule a tabletop exercise:** a walkthrough of a simulated incident using this plan, without touching live systems, at minimum annually and after any major system or team change.
2. **Assign a facilitator and a note-taker** to record exactly where the plan broke down or people hesitated.
3. **Update the plan** based on what the exercise surfaced, not just what worked.
4. **Log the exercise and its findings as evidence**, the same way a real incident's post-incident review is logged.

Date	Type (tabletop / real)	Scenario	Gaps found	Plan version updated

11. Sample Clauses

SAMPLE CLAUSE: SEVERITY CLASSIFICATION

Incidents are classified as Critical (confirmed unauthorized access to customer data, or a full production outage), High (suspected unauthorized access, or a partial service degradation), Medium (an internal-only anomaly with no confirmed customer or data impact), or Low (a policy violation with no active security risk). The incident commander assigns the initial severity within 15 minutes of a report and may revise it as more information becomes available.

SAMPLE CLAUSE: COMMUNICATION TREE (CRITICAL INCIDENT)

On confirmation of a Critical incident, the reporting party notifies the incident commander immediately. The incident commander notifies the technical lead and communications lead within 15 minutes. The communications lead notifies company leadership within 30 minutes and prepares any required customer or regulatory notification per the applicable framework's timeline. All notifications and timestamps are logged in the incident record as they happen.

Approval

Approved by	Title	Signature	Date

Produced by ComplyJet as a free companion to the [Incident Response Plan Template](#) guide. ComplyJet helps SaaS startups turn plans like this one into evidence-backed controls across SOC 1, SOC 2, ISO 27001, HIPAA, GDPR, PCI DSS, and 25+ other frameworks, including a place to log tabletop exercises and real incidents as evidence. [Book a free demo](#) to see how.