[Company name]

# Incident Response Plan

| | |
|---|---|
| **Owner** | [Security owner role] |
| **Approved by** | [Policy approver role] |
| **Effective date** | [Effective date] |
| **Next review** | [Next review date] |
| **Version** | [Version] |

## 1. Purpose and scope

This plan sets how [Company name] (the "Company") detects, responds to and learns from security incidents. It supports the SOC 2 common criteria CC7.3, CC7.4 and CC7.5 by establishing a formal process for managing security incidents.

This plan applies to all security and availability incidents affecting [In-scope systems] or the data they hold.

## 2. Severity

The incident lead sets the tier when the incident is declared, and raises it if the facts change. Each tier has a trigger anyone can apply and a clock.

| Tier | Trigger | Who is woken | Clock |
|---|---|---|---|
| SEV1 | Customer data reached by someone who should not have it, or production down for all | Incident lead, by phone, now | Contained same day, notice clock starts at declaration |
| SEV2 | A control failed and could have exposed data, or production degraded for some | Incident lead, within the hour | Contained same day, reviewed within five days |
| SEV3 | One account, device or dependency affected, and no data was reached | Ticket, next business day | Closed inside your stated remediation window |
| Not an incident | Scanner finding with no sign of use, failed login, phishing mail nobody clicked | Nobody | Vulnerability queue |

> Set clocks you will meet. Ticket timestamps are read against these numbers.

## 3. Roles

| Role | What it owns | Held by | Backup |
|---|---|---|---|
| Incident lead | Declares the tier, runs the response, calls the end | [Name] | [Name] |
| Technical response | Containment, evidence capture, the fix | [Name] | [Name] |
| Customer communication | Status page, customer notices, the contract clock | [Name] | [Name] |
| Record keeper | Timeline, decisions, timestamps | [Name] | [Name] |

At this size the incident lead and the technical responder are the same person below a SEV1, and every role names a backup. One person may hold several roles. No role is left without a name.

## 4. Response

The incident response process follows these phases:

1. Detection and reporting: Incidents are identified and logged in [Ticketing system].
2. Triage and containment: The impact is assessed and immediate steps are taken to limit damage.
3. Eradication and recovery: The root cause is removed and systems are restored.
4. Post-incident review: A blameless review is held for every incident within 5 business days, following section 6.

## 5. Notification

Internal and external stakeholders are notified of incidents according to their severity and impact, with a formal process for customer breach notification.

Affected customers, and any authority the law requires, are notified within [Notification deadline] of the incident being declared. That number is the shortest of the clocks below. The customer communication role sends every notice and records when it was sent.

| Where the clock comes from | Deadline | Applies to |
|---|---|---|
| Customer contracts and data processing addendums | [Hours] | [Customers with that clause] |
| Breach notification law | [Hours or days] | [Personal data, by jurisdiction] |
| Commitments the Company has published | [Hours] | [All customers] |

## 6. Post-incident review

Every incident gets a short written review, held within 5 business days. The record carries:

1. Detection time, and how the incident was detected: alert, customer report or someone noticing.
2. The tier, and whether it changed during the response.
3. A timeline with timestamps: detected, declared, contained, resolved and communicated.
4. Who was told, and when: customers, any authority that applies, and the internal record.
5. The root cause, and at least one action with an owner and a due date.

## 7. Annual exercise

The plan is exercised at least once a year, inside the audit period, with the people it names. A tabletop exercise is enough.

1. Pick a scenario the Company systems could produce, such as an API key committed to a public repository or a lost laptop.
2. Run it live for an hour: declare a tier, draft the customer notice and find the contract clock.
3. Write down what did not work.
4. Keep the record: date, attendees, scenario, findings, and actions with owners.

## 8. Evidence and records

The records below show that this policy operates. Each is dated, kept for at least [Evidence retention period], and stored where an auditor can be given it.

| Record | What it shows | Where it is kept |
|---|---|---|
| Approved policy | This document, signed by the approver, with its version history. | [Documentation system] |
| Incident log | Record of all security incidents. | [Ticketing system] |
| Post-incident reviews | The record in section 6 for each incident. | [Documentation system] |
| Exercise record | The annual tabletop or test, with attendees and actions. | [Evidence storage location] |
| Customer notices | Each notice sent, with the time it was sent. | [Evidence storage location] |

## 9. Exceptions and enforcement

A deviation from this policy needs a written exception approved by the [Security owner role] before it begins. Each exception records the rule not met, the business reason, the compensating control and an expiry date no more than 12 months away. Exceptions are reviewed at each annual review.

A breach of this policy is handled under the Company disciplinary process and may lead to action up to and including termination of employment or contract. A breach that exposes customer data is also handled as a security incident.

## 10. Review and approval

The [Security owner role] reviews this policy at least once a year and after any significant change to the business, the systems in scope or the risks they face. The [Policy approver role] approves each version. Personnel are told of material changes and acknowledge the current version.

| Version | Date | Summary of change | Approved by |
|---|---|---|---|
| [Version] | [Effective date] | First version. | [Policy approver role] |
| | | | |

**Policy approver**

Name:

Signature:

Date:

## 11. Fields to complete

Replace every bracketed field in this document with your own detail, then delete this section.

| Field | What to enter |
|---|---|
| [Company name] | Your legal company name. |
| [Effective date] | The date the approver signs this version. |
| [Version] | Start at 1.0 and increase it each time the document changes. |
| [Security owner role] | The role that runs the security program day to day, for example Chief Technology Officer. |
| [Policy approver role] | The officer who approves policies and accepted risks, for example Chief Executive Officer. |
| [Evidence storage location] | The shared folder or system where evidence is kept. |
| [Documentation system] | Where policies and procedures are published, for example the company wiki. |

| Field | What to enter |
| --- | --- |
| [In-scope systems] | The product, cloud accounts and tools inside the audit boundary. |
| [Ticketing system] | Where changes and incidents are tracked, for example Jira or Linear. |
| [Evidence retention period] | How long audit evidence is kept, for example three years. |
| [Notification deadline] | The shortest customer or legal notice period you are bound by, in hours. |
| [Next review date] | The date this version must be reviewed by, at most 12 months after the effective date. |

## Source

Source: free template from www.polaralabs.com/templates/incident-response-plan (CC BY 4.0).