

Security Incident Log

Owner	[Security owner role]
Kept in	[Ticketing system]
Covers	Every security event triaged and every security incident
Version	[Version]

1. How to use this log

This log is the one list of every security event [Company name] triaged and every security incident it handled. The Incident Response Plan says how an incident is run. This log is the record that it was. Keep one row per event, in the workbook or in [Ticketing system], and keep the same columns either way.

Open a row the moment an event is triaged, not when it is resolved. Fill in what is known, write Unknown where nothing is known yet, and update the row as the response moves. A row is never deleted. An event that turns out not to be an incident stays in the log at SEV4, because the row is the evidence that it was looked at.

Criterion	What it expects	What the log shows
CC7.3	Security events are evaluated to decide whether they are security incidents	Each event triaged and given a severity, including the ones closed as SEV4
CC7.4	Identified incidents are handled under a defined response: understood, contained, remediated and communicated	Containment, eradication, recovery and the customer notification decision for each incident
CC7.5	Activities to recover from identified incidents	Recovery, root cause and the post-incident review with its actions closed

2. The severity scale

Set the level at triage and raise it if the facts change. Each level has a trigger anyone on call can apply and a clock.

Level	Name	Trigger	Who is told	Clock
SEV1	Critical	Customer data reached by someone who should not have it, or production down for all customers	Incident lead by phone at once, then the executive who sends customer notices	Contained the same day. The customer notice clock starts when the incident is declared

Level	Name	Trigger	Who is told	Clock
SEV2	High	A control failed and could have exposed data, or production degraded for some customers	Incident lead within the hour	Contained the same day. Reviewed within five business days
SEV3	Moderate	One account, device or dependency affected, and no data was reached	A ticket, picked up the next business day	Closed inside the remediation window your policy states
SEV4	Event	A security event triaged and found not to be an incident: a scanner finding with no sign of use, failed sign ins, a phishing email nobody clicked	Nobody is woken. The row is the record of the triage	Closed at triage, or moved to the vulnerability queue

These four levels are the three tiers of the Incident Response Plan template plus its "not an incident" row. If your plan uses different levels, copy them here so the plan and the log never disagree.

3. What each column holds

Column	What to enter
Incident ID	A number that never repeats, for example INC-104. The same ID goes on the ticket, the review and any customer notice.
Detected on	The day the event was first seen, from the alert or the report, not the day someone opened the ticket.
Reported by	The person, customer, vendor or tool that raised it.
Detection source	Monitoring alert, staff report, customer report, vendor notice, third party report, or audit or review.
Severity	SEV1 to SEV4 from the severity scale. If the level changed during the response, write the final level and note the change in the summary.
Category	Unauthorized access attempt, unauthorized access, credential exposure, malware, phishing, data exposure, denial of service, lost or stolen device, vendor incident, misconfiguration, or other.
Systems affected	The systems named in your system inventory, not a general description.
Customer data affected	Yes, No or Unknown. Unknown is an honest answer while the facts are coming in. Change it once they are established, and say how.
Summary	Two or three sentences a reader outside the response can follow.
Containment action	What stopped the harm from spreading.

Column	What to enter
Contained at	When containment finished, counted from detection, for example same day, 35 minutes after the report.
Eradication	What removed the cause.
Recovery	What brought the affected systems back to normal operation.
Restored at	When normal operation resumed, counted from detection.
Root cause	The cause the review settled on, including any cause at a vendor.
Customer notification required	Yes, No or Under review, judged against your contracts, your published commitments and any law that applies.
Notification sent	The day the notice went out and who sent it, or Not required.
Post-incident review date	The day the written review was held. Every SEV1 to SEV3 incident gets one.
Owner	The role accountable for closing the row.
Status	Open, Contained, Resolved or Closed. Closed means every review action is done.

4. Worked example

Three rows from the log of Moonrake, a fictional ten person company that sells API security monitoring to fintech companies and runs on AWS. The full rows, with every column and two post-incident reviews, are in the workbook.

ID	Detected	Level	Category	Customer data	What happened and what was done	Notification	Status
INC-104	11 February	SEV3	Unauthorized access attempt	No	Okta push requests the engineer had not started, all denied. Sessions revoked, password reset, number challenge turned on.	Not required	Closed
INC-107	7 April	SEV2	Credential exposure	No	An AWS pipeline key in a pull request. Deactivated in 25 minutes, CloudTrail showed no other use, pipeline moved to short lived credentials.	Not required	Closed

ID	Detected	Level	Category	Customer data	What happened and what was done	Notification	Status
INC-112	12 August	SEV1	Vendor incident	Yes	The help desk vendor was breached and four tickets with customer contact details and one pasted API token were read. Token and integration key revoked.	Sent 14 August to the four customers	Closed

5. The post-incident review record

Every SEV1 to SEV3 incident gets a short written review within five business days. Record it on the Post-incident review sheet, or in the ticket, with:

1. The incident ID, the review date and who attended.
2. A timeline with times: detected, declared, contained, restored and, where it applies, customers notified.
3. How long it took to detect and to contain.
4. What worked and what did not.
5. The root cause.
6. At least one action, with an owner, a due date and the date it closed.

6. When there were no incidents

A period with no incidents still leaves a record. The log shows the events triaged and closed at SEV4, and management signs the statement below at the end of the period. Auditors read it beside the alert history and the tickets, so sign it only when the log supports it.

6.1 Statement of no security incidents

The management of [Company name] states that no security incidents, as the Incident Response Plan defines them, were identified during the period [Period start] to [Period end]. Every security event triaged during the period is recorded in the security incident log, at SEV4, with the triage decision.

[Signer name], [Signer title], [Company name]

Officer signing for management

Name:

Signature:

Date:

7. Keeping the records

- Keep the log, the tickets behind each row, the reviews and any customer notices for the period the Data Retention Policy sets for security records.
- Store them in [Evidence storage location], where an auditor can be given them, and restrict editing to the [Security owner role].
- Never edit a closed row to change what happened. Add a note with the date and the correction.

8. 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.
[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.
[Evidence storage location]	The shared folder or system where evidence is kept.
[Ticketing system]	Where changes and incidents are tracked, for example Jira or Linear.
[Period start]	For a Type 2 report, the first day of the period.
[Period end]	For a Type 2 report, the last day of the period.
[Signer name]	The officer signing for management.
[Signer title]	Their title, printed under the name.

Source

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