Security Incident Report Template

For internal security incident recording, review, follow-up and closure

How to use this template. Record what is known, distinguish observation from assumption, identify relevant evidence and make important unknowns visible. Immediate safety and incident response take priority over completing the form. Adapt this template to your organisation's procedures and terminology.

Important boundary. This form supports internal incident recording. It does not itself establish disputed facts, determine responsibility or replace any separate investigation, statutory, regulatory, police, client or sector-specific reporting requirement that may apply.

1. REPORT DETAILS

Organisation / site	*[Organisation and site/location]*
Incident reference	*[Unique incident reference]*
Report status	*[ ] Initial [ ] Updated [ ] Final*
Report date and time	*[DD/MM/YYYY, HH:MM]*
Reporter	*[Name, role and contact details]*
Incident classification / severity	*[Use the organisation's agreed classification, if applicable]*

2. INCIDENT DETAILS

Incident date and time	*[Known date/time. State if approximate.]*
Location	*[Exact location]*
Incident type	*[For example: unauthorised access, theft, violence, suspicious activity, damage]*
People involved	*[Names/identifiers if appropriate, or reference the People involved section below]*
Short summary	*[One or two factual sentences describing what is known to have happened]*

3. FACTUAL CHRONOLOGY

Record events in time order. Use precise times where known; otherwise state that the time is approximate. Identify the basis for each entry.

Date / time	What happened	Basis / source
[HH:MM]	*[Factual event or action]*	*[Observed / reported by / CCTV / access record / other]*

4. PEOPLE INVOLVED

Record only information needed for the incident record and handle personal information in line with your organisation's requirements.

Name / description	Role or relationship	Involvement / relevant information	Contact / reference
[Name or description]	*[Employee / visitor / contractor / witness / other]*	*[Factual involvement]*	*[Contact or internal reference, if appropriate]*

5. IMPACT AND IMMEDIATE RESPONSE

Immediate impact / consequences	*[Record injury or welfare concerns, unauthorised access, loss, damage, disruption, affected controls, information/data impact or other consequences. If none were identified, state what was checked.]*
Immediate actions taken	*[Record action taken during or immediately after the incident, including by whom and when where relevant.]*
Current position	*[What is the position now? What has been checked? What remains unresolved? Avoid broad conclusions that are not supported.]*

6. EVIDENCE AND REFERENCES

Identify and reference relevant evidence. Keep controlled material in its authorised location rather than copying it into the report unnecessarily.

Reference	Type	Where held	Relevant period / detail	Retention / preservation action
[Ref]	*[CCTV / photo / access record / statement / log / other]*	*[System/location]*	*[Time range, file or record detail]*	*[Action taken, if applicable]*

7. NOTIFICATIONS AND ESCALATION

Record internal and external notifications made. Consider separately whether any police, emergency, client, insurer, regulatory or sector-specific reporting requirement applies.

Date / time	Person / organisation	Reason / type	Action or reference	Completed by
[HH:MM]	*[Name / organisation]*	*[Internal / police / client / regulator / other]*	*[Outcome or reference]*	*[Name / initials]*

8. OUTSTANDING QUESTIONS / UNKNOWNS

Do not fill gaps with assumptions. Record material questions that remain unanswered and who, if anyone, is responsible for checking them.

Question / unknown	Owner	Target date	Status / outcome
[What has not yet been established?]	*[Owner, if applicable]*	*[Date]*	*[Open / resolved / not pursued + reason]*

9. FOLLOW-UP ACTIONS

Action	Owner	Due date	Status	Outcome / evidence
[Specific action]	*[Named owner]*	*[Date]*	*[Open / in progress / complete]*	*[Evidence of completion or outcome]*

10. REVIEW, LESSONS AND RECOMMENDATIONS

What should change?	*[Record any justified change to controls, procedures, briefing, training, equipment, staffing or other arrangements.]*
Could the same issue exist elsewhere?	*[Consider other locations, teams, shifts, sites or processes.]*
Has something similar happened before?	*[Reference previous incidents, trends or records where relevant.]*
Lessons to retain or share	*[Record any lesson that should inform future briefings, procedures, reviews or decisions.]*
Recommendations	*[Record recommendations that require a decision. Where accepted, convert them into owned follow-up actions above.]*

11. REVIEW AND CLOSURE

Reviewed by	*[Name and role]*
Date reviewed	*[DD/MM/YYYY]*
Further action required?	*[ ] Yes [ ] No If yes, ensure actions are recorded above.*
Closure date	*[DD/MM/YYYY]*
Closure comments	*[Record why the incident can be closed, any remaining accepted risk, and where the final record is retained.]*
Closed by	*[Name and role]*

Before closure. Check that the chronology is understandable, observations are distinguished from assumptions, relevant evidence is referenced, important unknowns are visible, required notifications have been considered, and accepted actions have owners and outcomes.

Template version: August 2026