COMPANION DOCUMENT

Incident response records

Ten templates for PIVTR-D, an incident response operating guide, version 2.0.

Habib Tora | September 2026

Produce these during the incident rather than after it. Reconstructing a timeline from chat history three weeks later takes longer and produces a worse record. Each template is a plain text form: copy it into the incident ticket, or fill it in here and attach it.

Waypoint	Record
V and T. Verification and triage	T1 incident record, T2 triage brief
R. Response (contain)	T3 containment decision record
R. Response loop	T4 iteration log, T5 technical closure, T6 residual risk acceptance
R. Response (recover)	T7 pre-restoration sign-off, T8 system owner acceptance
D. Debrief	T9 after-action review agenda, T10 executive debrief

T1. Incident record, opened at verification

```
INCIDENT ID        :
TITLE              :
HANDLER            :
REPORTED           :           (date, time, zone)
REPORT SOURCE      :           user | alert | partner | hunt | third party
CLASSIFICATION     :           unauthorized access | phishing | malicious code |
                               data disclosure | account compromise |
                               public-facing exploit | other
INITIAL RISK       :           low | medium | high | critical
SUMMARY            :

EVIDENCE REFS      :

VERIFY DECISION    :           continue | stop | defer
RATIONALE          :
DECIDED BY / AT    :
```

T2. Triage brief to decision makers

```
INCIDENT ID        :
AS OF              :           (time of this brief)

WHAT WE KNOW       :           (facts only, three lines maximum)
  1.
  2.
  3.
```

```
WHAT WE DO NOT KNOW:
  1.
  2.

SYSTEMS IN SCOPE   :            (counts by class: servers, workstations, cloud, identities)
BUSINESS EXPOSURE  :            revenue | regulated data | safety | contractual
PROPOSED POSTURE   :            passive | adaptive | active | deceptive

ACTION REQUESTED   :            (the one authorization you need)
IF APPROVED        :            (impact)
IF DEFERRED        :            (impact)

DECISION / BY / AT :
```

T3. Containment decision record

```
INCIDENT ID        :
ACTION             :
SYSTEMS / ACCOUNTS :
LAYER              :            network | host | application | identity
TRIGGER            :            active destruction | exfiltration | safety |
                                regulatory clock | judgment call

POSTURE            :            passive | adaptive | active | deceptive
AUTHORIZED BY      :            (per authority matrix)
BUSINESS IMPACT    :            (assessed before execution)
EXECUTED AT        :            (simultaneous across teams where possible)
ROLLBACK PROCEDURE :

VALIDATION
  network          :            pass | fail  -  what was checked
  process          :            pass | fail  -  what was checked
  logs             :            pass | fail  -  what was checked
VALIDATED BY / AT  :
```

T4. Loop iteration log

```
INCIDENT ID        :
ITERATION #        :
OPENED AT          :
TRIGGER TYPE       :            new indicator | scope expansion |
                                incomplete eradication | analysis revelation |
                                business change
TRIGGER DETAIL     :

CHANGES TO
  scope            :
  containment      :
  eradication      :
  recovery         :

NEW INDICATORS     :
CLOSED AT          :
CARRIED FORWARD    :            (what the next iteration inherits)
```

T5. Technical closure

```
INCIDENT ID        :
ITERATIONS RUN     :

No new indicators in scoping since   :
Monitoring clean since               :
Eradication verified                 :   method / analyst / date
Restored systems nominal since       :
Outstanding visibility gaps          :
Monitoring retained, and for how long:

TECHNICAL CLOSURE BY :          (name, role)
DATE / TIME          :
```

T6. Residual risk acceptance

```
INCIDENT ID        :

RESIDUAL RISKS ACCEPTED        (one line each, plain language)
  1.
  2.
  3.

COMPENSATING CONTROLS RETAINED :
CONDITIONS THAT WOULD REOPEN   :
  1.
  2.

ACCEPTED BY        :            (name, role - the risk owner, not the IR team)
DATE / TIME        :
```

T7. Pre-restoration sign-off

```
INCIDENT ID        :          SYSTEM :

CHECK                          RESULT    BY        DATE
1 Root cause remediated        pass/fail
2 Patching current             pass/fail
3 Persistence removed          pass/fail
4 Backup predates compromise   pass/fail/na
5 Rebuild from trusted media   pass/fail/na
6 EDR, firewall, logging live  pass/fail
7 Indicator scan (run last)    pass/fail

EXCEPTIONS ACCEPTED :
VERIFIED BY / AT    :
```

T8. System owner acceptance

```
INCIDENT ID        :          SYSTEM :
OWNER              :

TESTS PERFORMED    :
PERFORMED BY       :
ISSUES FOUND       :
```

```
LIMITATIONS ACCEPTED BY OWNER  :
ENHANCED MONITORING CONFIRMED  :   yes | no
DETECTION RULES ENABLED        :   yes | no

OWNER SIGN-OFF     :            (name, role)
DATE / TIME        :
```

T9. After-action review agenda, 90 minutes

```
INCIDENT           :          DATE :
ATTENDEES          :            (every team that took part)

0:00  Ground rules. Blameless. Controls, procedures, resources.
      Individual performance is handled elsewhere.
0:05  Timeline walkthrough (prepared in advance)
0:30  What worked, and why
0:45  What slowed us down
1:05  Root cause, and the organizational conditions behind it
1:20  Candidate improvements, ranked by risk reduction
1:30  Owners and dates assigned

DECISIONS          :
IMPROVEMENTS + OWNERS + DATES   :
  1.
  2.
  3.
```

T10. Executive debrief, one page

```
INCIDENT           :          DATE :
CLASSIFICATION     :          SEVERITY :

WHAT HAPPENED      :            (three sentences, no jargon)

IMPACT
  systems          :
  accounts         :
  records / data   :
  downtime         :
  cost to date     :

HOW IT ENDED       :
ROOT CAUSE         :

WHAT WE ARE CHANGING            (owner and date on each)
  1.
  2.
  3.

WHAT WE NEED       :            (funding, staff, policy - ask now)
```