Post-Incident Review and Reporting Framework

1. Incident Summary

Brief Description of the Incident:

Describe the incident succinctly.

Date & Time of Incident:

YYYY-MM-DD HH:MM

Location / System Affected:

E.g., Main Server Room, Application Name

2. Incident Details

Impact Assessment:

Outline impact - Services affected, Users impacted, Duration, etc.

How Incident Was Detected:

Who/what detected the issue and how.

Incident Timeline:

Time	Event / Action
HH:MM	Description of event/action
HH:MM	Description of event/action

3. Root Cause Analysis

Identified Root Cause(s):

Summarize investigation findings and main causes.

Contributing Factors:

List any factors, processes, or issues that worsened the incident.

4. Response & Recovery

Actions Taken (by whom):

Detail steps taken to resolve/recover from the incident.

Internal and External Communications:

Summarize notifications, escalations, or customer communications.

5. Lessons Learned & Recommendations

Key Lessons Learned:

What worked well, what could be improved.

Recommendations for Prevention:

Actions to prevent recurrence, process improvements, training, etc.

6. Follow-Up Actions

Action Item	Responsible	Target Date	Status
Action to be taken	Person/Team	YYYY-MM-DD	Open/Closed
Action to be taken	Person/Team	YYYY-MM-DD	Open/Closed

7. Review & Approval

Reviewed By:

Name / Position

Date Reviewed:

YYYY-MM-DD