**Post-Incident Analysis Report Template**

**1. Incident Overview**

* Incident ID:
* Date & Time of Incident:
* Date & Time Detected:
* Duration of Incident:
* Reported By:
* Location / Affected Systems:

**2. Description of Incident**

* Summary of What Happened:
* Type of Incident: (e.g., Phishing, Malware, Unauthorized Access)
* Attack Vector: (e.g., Email, Web Application, USB device)
* Impact Level: (Low, Medium, High, Critical)
* Affected Parties: (e.g., internal users, customers, vendors)

**3. Timeline of Events**

|  |  |
| --- | --- |
| **Time (UTC)** | **Event Description** |
| 10:00 | Suspicious login detected |
| 10:30 | Alert triggered in SIEM |
| 11:00 | Incident Response Team engaged |

**4. Root Cause Analysis**

* Root Cause Identified:
* How and Why Did It Happen?
* Detection Gaps / Failures:

**5. Containment, Eradication, and Recovery**

* Containment Actions Taken:
* Eradication Steps:
* Systems Restored:
* Recovery Timeline:
* Verification of Restoration Success:

**6. Communication and Coordination**

* Internal Communications:
* External Notifications: (e.g., regulators, affected customers)
* Press or Public Statement: (if applicable)

**7. Lessons Learned**

* What Went Well:
* What Could Have Been Done Better:
* Breakdowns in Process or Communication:
* Tools or Procedures That Need Improvement:

**8. Action Items and Recommendations**

|  |  |  |  |
| --- | --- | --- | --- |
| **Action Item** | **Owner** | **Due Date** | **Status** |
| Patch vulnerable systems | IT Security | MM/DD/YYYY | In Progress |
| Update incident response playbook | CISO | MM/DD/YYYY | Not Started |

**9. Supporting Evidence and Attachments**

* Logs
* Screenshots
* Emails
* Network Maps
* Tools Used (e.g., forensics tools)

**10. Approval & Sign-off**

* Report Prepared By:
* Reviewed By:
* Approved By:
* Date of Sign-off: