# Incident Response Starter Kit

**1. Incident Response Flowchart**

A comprehensive step-by-step guide to responding to incidents effectively, ensuring no critical steps are missed.

**Flowchart Details:**

1. **Detection & Identification**
   * **Inputs:** Monitoring tools, user reports, suspicious activity logs.
   * **Actions:**
     + Activate incident response team.
     + Classify incident severity (Low, Medium, High, Critical).
     + Confirm whether it’s a real incident or a false positive.
2. **Containment (Immediate and Long-Term)**
   * **Short-Term Actions:**
     + Disconnect affected systems from the network.
     + Disable compromised accounts.
   * **Long-Term Actions:**
     + Apply temporary fixes to stop the spread.
     + Preserve system state for forensic analysis.
3. **Analysis**
   * **Inputs:** Logs, network traffic data, endpoint detection reports.
   * **Actions:**
     + Determine the origin, attack vector, and scope.
     + Identify attackers’ tools, tactics, and procedures (TTPs).
     + Prioritize systems/assets based on criticality.
4. **Communication**
   * **Stakeholders:** Internal teams, leadership, legal, regulatory bodies, customers (if applicable).
   * **Actions:**
     + Create a communication plan.
     + Avoid speculation; focus on facts.
     + Coordinate with external cybersecurity and legal partners if needed.
5. **Eradication**
   * **Actions:**
     + Remove malware, unauthorized access, or malicious code.
     + Patch vulnerabilities.
     + Confirm removal through retesting systems.
6. **Recovery**
   * **Actions:**
     + Restore systems from clean backups.
     + Monitor systems for anomalies.
     + Validate recovery with testing.
7. **Post-Incident Review**
   * **Actions:**
     + Conduct a root-cause analysis.
     + Document incident handling details.
     + Update incident response policies and training materials.
     + Implement new security controls to prevent recurrence.

**2. Incident Log Template**

A detailed template for recording all critical information related to security incidents.

| **Field** | **Description** | **Example** |
| --- | --- | --- |
| **Date & Time** | When the incident was first detected and logged. | 2024-12-18 14:35 |
| **Incident Type** | Specify the type of incident (e.g., malware, phishing, insider threat, system misconfiguration). | Ransomware attack |
| **Detected By** | Name or system that identified the incident. | Jane Doe (System Admin), SIEM Alert #12345 |
| **Description** | Brief overview of the incident. | Unusual outbound traffic detected from Server X. |
| **Affected Systems** | List of impacted systems, users, or networks. | Finance Server X, user accounts for John Doe and Sarah Lee. |
| **Actions Taken** | Steps performed to contain or mitigate the incident. | Isolated server, disabled compromised accounts, alerted incident response team. |
| **Evidence Collected** | Details of logs, screenshots, or forensic data gathered. | Firewall logs, memory dumps, endpoint protection alerts. |
| **Root Cause** | Analysis of how the incident occurred and key vulnerabilities exploited. | Outdated software patch allowed exploitation via known CVE. |
| **Resolution** | Final status after containment, eradication, and recovery. | Malicious software removed; system restored; updated patches applied. |
| **Follow-Up Actions** | Actions needed to strengthen defenses and prevent recurrence. | Enforce MFA, update patch management processes, retrain employees on phishing awareness. |
| **Logged By** | Name/role of the individual recording the incident. | John Smith (Incident Response Specialist) |

**3. Contact List Template**

A detailed template for internal and external contacts to be used during an emergency.

| **Contact Type** | **Name/Role** | **Phone Number** | **Email** | **Notes** |
| --- | --- | --- | --- | --- |
| **Internal Contacts** |  |  |  |  |
| IT Support | John Doe (IT Lead) | +1-555-123-4567 | john.doe@company.com | Primary POC for system issues. |
| Incident Lead | Jane Smith (IR Manager) | +1-555-987-6543 | jane.smith@company.com | Responsible for coordinating IR. |
| CISO | Mark Johnson | +1-555-222-3333 | mark.johnson@company.com | Escalation for critical incidents. |
| HR Team | Susan Lee | +1-555-444-5555 | hr@company.com | For insider threats or employee-related issues. |
| **External Contacts** |  |  |  |  |
| Legal Counsel | ABC Law Firm (Data Privacy) | +1-800-111-2222 | privacy@abclaw.com | Legal guidance on breaches. |
| Cybersecurity Partner | DEF Security Solutions | +1-800-333-4444 | response@defsecurity.com | Assistance with forensic analysis. |
| Regulatory Body | Data Protection Authority | +1-800-555-7777 | breach@regulatory.gov | Report required for compliance breaches. |
| Law Enforcement | Cybercrime Division | +1-800-999-8888 | cybercrime@police.gov | For criminal investigations. |

**Additional Notes:**

* Always validate contact information regularly to ensure it is up-to-date.
* Maintain both electronic and hard copies in secure, easily accessible locations.

**4. Additional Resources**

* **Incident Response Policy**: Maintain a detailed policy document that aligns with your organization’s security requirements.
* **Training Schedule**: Regular training for staff on recognizing and reporting incidents.