The **NIST Incident Response Framework** is outlined in **NIST Special Publication 800-61 Rev. 2** and consists of four key phases:

1. **Preparation**
2. **Detection & Analysis**
3. **Containment, Eradication & Recovery**
4. **Post-Incident Activity**

Incident Response Report (NIST-Based Template)

1. Incident Summary

- **Incident Name:** [Short identifier, e.g., "Ransomware Attack - HR Server"]
- **Date & Time of Detection:** [YYYY-MM-DD HH:MM]
- **Reported By:** [SOC Analyst, Employee, System Alert, etc.]
- **Incident Category:** [Malware, Phishing, Data Breach, DDoS, Insider Threat, etc.]
- **Incident Severity Level:** [Low | Medium | High | Critical]
- **Affected Assets:**
    - Systems: [List impacted systems, e.g., HR-SERVER-01]
    - Users: [List affected users or departments]

2. Preparation

- **Incident Response Team (IRT) Members & Roles:**
    - Incident Manager: [Name]
    - SOC Analyst: [Name]
    - Threat Intelligence Analyst: [Name]
    - IT Support: [Name]
- **Security Measures in Place:**
    - Firewalls, IDS/IPS, Endpoint Detection & Response (EDR) tools
    - Patch management status
    - Security awareness training details
- **Communication Plan:**
    - Internal escalation contacts
    - External reporting obligations (if applicable, e.g., GDPR, CISA, etc.)

3. Detection & Analysis

- **Detection Method:**
    - System Alert (SIEM, Firewall, IDS/IPS)
    - Employee Report
    - Threat Intelligence Feed
- **Initial Indicators of Compromise (IOCs):**
    - Suspicious files/processes detected
    - IP addresses involved
    - Malware hashes (MD5, SHA256)
    - Unauthorized logins
- **Log Analysis & Investigation Findings:**
    - Source of attack: [External, Insider, Supply Chain, etc.]
    - Attack vector: [Phishing, Exploit, Credential Compromise, etc.]
    - Timeline of Events:
        - **T0:** [Initial compromise timestamp]
        - **T1:** [First lateral movement]
        - **T2:** [Data exfiltration detected]
- **Impact Assessment:**
    - **Data Compromised:** [PII, Intellectual Property, Financial Data, etc.]
    - **Operational Impact:** [System downtime, Business interruption]

4. Containment, Eradication & Recovery

Containment

- **Short-Term Actions:**
    - Disconnect affected systems? [Yes/No]
    - Block malicious IPs/domains? [Yes/No]
    - Reset compromised credentials? [Yes/No]
- **Long-Term Actions:**
    - Patch vulnerabilities? [Yes/No]
    - Increase monitoring? [Yes/No]
    - Restrict access to critical assets? [Yes/No]

Eradication

- **Root Cause Identified?** [Yes/No]
- **Threat Removal Steps Taken:**
    - Removed malware/backdoors? [Yes/No]
    - Applied security patches? [Yes/No]
    - Enhanced security controls? [Yes/No]

Recovery

- **Restoration Steps:**
    - Restored affected systems from backups? [Yes/No]
    - Conducted security validation? [Yes/No]
    - Monitored for reinfection? [Yes/No]
- **Downtime Duration:** [HH:MM]
- **Final Security Check Before Going Live:** [Yes/No]

5. Post-Incident Activity

- **Lessons Learned:**
    - What worked well?
    - What needs improvement?
    - Were there any gaps in detection or response?
- **Future Preventive Measures:**
    - Strengthen security controls? [Yes/No]
    - Improve user awareness training? [Yes/No]
    - Enhance monitoring and logging? [Yes/No]
- **Incident Report Closure Date:** [YYYY-MM-DD]
- **Reviewed By:** [Security Team, IT Management, Compliance Officer]