# Incident Response Playbook (NIST 800-61)

This playbook provides standardized response procedures for cybersecurity incidents using the NIST Special Publication 800-61 Computer Security Incident Handling Guide. It includes end-to-end processes for two incident types: phishing compromise and ransomware infection.

## 1. Preparation
- Define roles and responsibilities.
- Ensure logging and monitoring are active (Windows Event Logs, SIEM, endpoint tools).
- Maintain an updated contact list for internal teams (IT, Security, Legal, HR, Management).
- Confirm backup procedures, offline backups, and system images.
- Train users on phishing awareness and secure authentication practices.
- Validate MFA enforcement and password policies.
- Maintain incident response toolkit (Sysinternals, Wireshark, forensics tools, scripts).

## 2. Detection & Analysis
- Validate initial alert from user report, email security tools, SIEM, or EDR system.
- Identify indicators of compromise (IOCs):
  - Suspicious IP addresses
  - Malicious domains/URLs
  - Hashes of malicious files
  - Unusual login locations
- Triage severity:
  - **Low** – Contained, no privileged access
  - **Medium** – Lateral movement attempt
  - **High** – Privileged account compromised or encryption detected
- Collect evidence:
  - Event logs
  - Network captures
  - Email headers
  - Process lists
  - Authentication logs
- Document timeline of events.

## 3. Containment
- Short-term containment:
  - Isolate impacted host from the network.
  - Disable compromised accounts.

  - Block malicious IPs/domains at the firewall.
- Long-term containment:
  - Apply patches if needed.
  - Strengthen account policies.
  - Reset VPN, AD, cloud, or email credentials.
  - Monitor access logs for reinfection attempts.

## 4. Eradication
- Remove malicious files, registry keys, scheduled tasks, or persistence mechanisms.
- Uninstall rogue applications or browser extensions.
- Patch exploited vulnerabilities.
- Flush DNS cache, reset browser settings, or wipe infected devices.
- Restore clean system configuration.

## 5. Recovery
- Reconnect systems to the network after validation.
- Restore data from clean backups if needed.
- Verify that logs show no continued malicious activity.
- Monitor affected systems for 24–72 hours.
- Re-enable user accounts with stronger authentication.

## 6. Lessons Learned
- Conduct a post-incident review within 72 hours.
- Analyze root cause, impact, and response effectiveness.
- Update security policies, monitoring rules, and training materials.
- Adjust playbook based on gaps discovered during the incident.

# INCIDENT SCENARIOS
This playbook includes two detailed scenarios:

1. **Phishing Compromise**
2. **Ransomware Attack**

Each scenario includes:
- Incident overview
- Detection indicators

- Containment & eradication steps
- Recovery plan
- Escalation process
- MITRE ATT&CK mapping
- IOC tables