**Standard Operating Procedure (SOP)**

**Organization Name:** Cyber Defense Force (Simulated Organization)  
**Title:** Cyber Operations SOP – Incident Response  
**Version:** 1.0  
**Date:** December 10, 2024

**1. Purpose**

To standardize the approach to detecting, responding to, and recovering from cybersecurity incidents, ensuring minimal impact on operations and compliance with regulatory standards.

**2. Scope**

This SOP applies to all members of the Cyber Defense Force, including employees, contractors, and third-party vendors, involved in monitoring, responding to, and reporting cybersecurity incidents.

**3. Roles and Responsibilities**

* **Cyber Operations Manager:**
  + Oversee all incident response activities and approve remediation steps.
  + Serve as the point of contact for executive briefings.
* **Incident Responder:**
  + Analyze alerts, contain threats, and mitigate vulnerabilities.
  + Document all actions during incident response.
* **Compliance Officer:**
  + Ensure incident response activities comply with NIST and DoD standards.
  + Maintain an audit trail of all incidents and responses.

**4. Procedure**

**Step 1: Detection and Reporting**

1. Monitor the SIEM dashboard for real-time alerts (e.g., Splunk, SolarWinds).
2. When an alert triggers:
   * Validate the alert by cross-referencing system logs.
   * Log the incident in the Cyber Defense Incident Tracker within 15 minutes of detection.
   * Notify the Cyber Operations Manager if the alert is classified as "High" or "Critical."

**Step 2: Triage and Classification**

1. Assign a severity level:
   * **Low:** Minimal risk, no operational impact.
   * **Medium:** Moderate risk with potential operational impact.
   * **High:** Immediate operational impact or sensitive data risk.
   * **Critical:** Threat to multiple systems or regulatory compliance.
2. Escalate all "High" or "Critical" incidents to the Incident Response Team for immediate action.

**Step 3: Containment**

1. Disconnect affected devices from the network.
2. Implement temporary firewall rules to block identified malicious IPs.
3. Disable user accounts suspected of compromise.

**Step 4: Mitigation and Eradication**

1. Remove malicious files, scripts, or processes using forensic tools (e.g., FTK, CrowdStrike).
2. Patch affected systems with security updates.
3. Review configurations to ensure the vulnerability is fully remediated.

**Step 5: Recovery**

1. Restore data and systems from verified backups.
2. Test restored systems for normal operations.
3. Reconnect the recovered system to the network after approval from the Cyber Operations Manager.

**Step 6: Post-Incident Reporting**

1. Complete the **Incident Response Report**, including:
   * Incident timeline.
   * Root cause analysis.
   * Actions taken and lessons learned.
2. Submit the report to the Compliance Officer within 24 hours of incident closure.
3. Schedule a follow-up meeting to discuss improvements in processes and technology.

**5. Compliance Requirements**

This SOP complies with:

* **NIST Cybersecurity Framework:** Identify, Detect, Respond, Recover.
* **DoD 8140.03 Standards:** Advanced Incident Response Procedures.
* **Federal Information Security Management Act (FISMA):** Incident handling guidelines.

**6. Tools and Resources**

* **SIEM Tools:** Splunk, SolarWinds.
* **Vulnerability Scanners:** OpenVAS, Nessus.
* **Backup Solutions:** Veeam, Acronis.
* **Forensic Tools:** FTK, EnCase.

**7. Appendices**

**Appendix A: Incident Report Template**

* **Incident ID:** [Unique Identifier]
* **Severity Level:** [Low, Medium, High, Critical]
* **Summary:** [Brief Description of the Incident]
* **Root Cause:** [Description of Root Cause]
* **Timeline:** [Start and End Time of Incident]
* **Actions Taken:** [Containment, Mitigation, Recovery Steps]
* **Lessons Learned:** [Key Insights for Process Improvement]

**Appendix B: Workflow Diagram**

* **Flowchart:**

plaintext

Copy code

Monitor SIEM --> Validate Alert --> Log Incident --> Triage & Classify -->

If High/Critical --> Notify Manager & Contain --> Mitigate -->

Restore Systems --> Post-Incident Reporting --> Improve Processes