**Draft Template**

**Standard Operating Procedure (SOP)**

**Organization Name:** [Your Simulated Organization Name]  
**Title:** Cyber Operations SOP – Incident Response  
**Version:** 1.0  
**Date:** [Insert Date]

**1. Purpose**

To provide a standardized approach to responding to cybersecurity incidents to minimize impact and restore operations efficiently.

**2. Scope**

Applies to all employees and contractors involved in incident detection, response, and reporting.

**3. Roles and Responsibilities**

* **Cyber Operations Manager:**
  + Oversee the incident response process.
  + Approve post-incident reports.
* **Incident Responder:**
  + Investigate, contain, and mitigate incidents.
  + Document actions taken during the response.
* **Compliance Officer:**
  + Ensure all actions comply with regulations.

**4. Procedure**

**Step 1: Detection and Reporting**

* Monitor SIEM for alerts.
* Log the incident in the tracking system within 15 minutes of detection.

**Step 2: Triage and Classification**

* Analyze the alert to determine the severity level (Low, Medium, High, Critical).
* Escalate incidents classified as "High" or "Critical" to the Cyber Operations Manager.

**Step 3: Containment**

* Isolate affected systems from the network.
* Implement temporary firewall rules to block malicious traffic.

**Step 4: Mitigation and Eradication**

* Remove malicious files or scripts.
* Apply patches or updates to affected systems.

**Step 5: Recovery**

* Restore systems from backups.
* Test restored systems to verify functionality.

**Step 6: Post-Incident Reporting**

* Complete the Incident Response Report.
* Submit the report to the Compliance Officer within 24 hours.

**5. Compliance Requirements**

This SOP aligns with:

* NIST Cybersecurity Framework: Detect, Respond, Recover.
* DoD 8140.03 standards for incident response.

**6. Tools and Resources**

* SIEM: [Insert Tool Name]
* Vulnerability Scanner: [Insert Tool Name]
* Backup Solution: [Insert Tool Name]

**7. Appendices**

* **Appendix A:** Incident Report Template.
* **Appendix B:** Workflow Diagram for Incident Response.

**Next Steps**

1. **Add Realistic Scenarios:** Customize the SOP with a specific example incident (e.g., phishing attack, ransomware).
2. **Create Flowcharts:** Use Lucidchart to create visual workflows for the steps.
3. **Review for Completeness:** Ensure all roles, steps, and tools are covered.