Endpoint Compromise Response Sheet

Incident Overview

Incident ID	
Date & Time Detected	
Reported By	
Endpoint Name / ID	
Location	
Owner / User	

Description of Compromise

Summary:

Indicators of Compromise (IoC):

Initial Actions Taken

- Isolate endpoint from the network:
- Capture volatile memory/image:
- Collect relevant logs/artifacts:
- Other (specify):

Investigation

Suspected Entry Point:

Malicious Activity Observed:

Accounts Impacted:

Scope of Compromise:

Containment, Eradication, and Recovery

Containment Steps:

Eradication Steps:

Recovery Steps:

Post-Incident Actions

- Reset passwords:
- Update security controls/rules:
- Vulnerability remediation:
- User notification/training:
- Review/update incident response plan:

Lessons Learned

Approval & Sign-off

Name	Role	Date	Signature