Incident Containment and Eradication Guideline

1. Purpose

This document provides step-by-step guidelines for the containment and eradication of detected security incidents to minimize impact and restore normal operations as quickly as possible.

2. Scope

These procedures apply to all systems, networks, and data under the organization's control that may be affected by a security incident.

3. Containment

1. **Short-Term Containment**
    - Isolate affected systems from the network, if possible.
    - Change relevant access credentials immediately.
    - Preserve volatile data for investigation (e.g., memory captures, logs).
    - Disable compromised user or system accounts temporarily.

2. **Long-Term Containment**
    - Apply temporary system controls (e.g., firewall rules) to prevent attacker movement.
    - Patch vulnerabilities related to the incident.
    - Implement increased system monitoring.

4. Eradication

1. Identify and remove all malicious files, software, or unauthorized changes.
2. Remove backdoors or persistence mechanisms discovered during investigation.
3. Apply system and security patches as required.
4. Update and harden affected system configurations.
5. Confirm the integrity of affected data and systems.

5. Roles and Responsibilities

Role	Responsibility
Incident Response Team	Lead containment and eradication activities and communicate status updates.
System Administrators	Assist in isolating and restoring affected systems.
IT Management	Authorize major containment or eradication actions as required.

6. Documentation

- Document all containment and eradication steps taken.
- Retain relevant logs and evidence for forensic review.
- Record lessons learned and update response procedures as appropriate.

7. References

- Incident Response Policy
- NIST SP 800-61: Computer Security Incident Handling Guide