Incident Containment and Mitigation Guide

1. Purpose

This guide outlines the steps for the containment and mitigation of security incidents to minimize potential impact and restore normal operations as quickly as possible.

2. Scope

Applies to all employees, contractors, and third parties involved in incident response procedures across the organization.

3. Incident Containment Steps

1. **Identify** affected systems and scope of the incident.
2. **Isolate** compromised systems from the network.
3. **Preserve Evidence:** Document actions taken, collect relevant logs and data.
4. **Assess** containment options (e.g., temporary or permanent isolation).
5. **Implement** containment measures with minimal disruption to business functions.
6. **Verify** containment is effective and contains lateral movement.

4. Mitigation Procedures

1. Remove or disable malicious components (e.g., malware, unauthorized accounts).
2. Apply patches and security updates where applicable.
3. Restore systems from known good backups if necessary.
4. Monitor systems for recurring or related activity.
5. Communicate updates to stakeholders as appropriate.

5. Roles and Responsibilities

Role	Responsibility
Incident Response Team	Lead containment and mitigation activities, coordinate with stakeholders.
IT Operations	Assist in isolating and restoring systems.
Management	Approve significant actions, communicate with executive leadership.

6. Communication

- Report progress to relevant business units and leadership.
- Maintain records of containment and mitigation steps.
- Escalate unresolved issues according to the incident escalation process.

7. Post-Incident Actions

1. Review containment and mitigation effectiveness.
2. Update documentation and procedures as needed.
3. Conduct a lessons learned meeting.

8. References

- Incident Response Policy
- Business Continuity Plan