SOP: Incident Identification and Initial Response Procedures

This SOP details the **incident identification and initial response procedures**, covering the steps to recognize potential incidents promptly, assess the situation for safety hazards, initiate immediate response actions, notify appropriate personnel, and document the incident accurately. The objective is to ensure a swift and effective reaction to minimize harm, contain damage, and support subsequent investigation and resolution efforts.

1. Purpose

To establish a standardized process for the prompt identification of incidents and ensure an immediate and controlled response to reduce potential harm or impact.

2. Scope

This procedure applies to all staff members, contractors, and third-party personnel across all organizational locations and operational domains.

3. Definitions

Term	Definition
Incident	An unplanned event or occurrence that may result in harm, disruption, or loss.
Initial Response	The first actions taken to assess, contain, and manage an incident.

4. Responsibilities

- **All Employees:** Remain vigilant, report observed or suspected incidents immediately, and cooperate with investigations.
- **Supervisors/Managers:** Lead the assessment, notify appropriate parties, ensure accurate documentation.
- **Incident Response Team/Security:** Provide guidance, contain threats, support investigation and resolution.

5. Procedure

1. **Incident Detection and Recognition**
    - Remain alert for any signs of anomalies, breaches, safety hazards, or malicious activities.
    - If an incident is suspected or identified, **do not ignore** or delay action.
2. **Immediate Safety Assessment**
    - Determine if there is any immediate risk to health, life, or critical infrastructure.
    - If urgent danger exists, activate emergency protocols (e.g., evacuation, medical aid, fire alarms).
3. **Initial Containment Actions**
    - Take steps to contain the incident without exposing oneself or others to unnecessary risk.
    - If appropriate, isolate affected systems or areas (e.g., disconnect network devices, restrict access).
4. **Notification**
    - Immediately report the incident to your supervisor, security, and/or the designated Incident Response Team.
    - Provide key details: time detected, nature of the incident, affected areas, initial actions taken.
5. **Documentation**
    - Record all relevant information about the incident and actions taken, including times and personnel involved.
    - Use the Incident Report Form or organizational reporting system as required.
6. **Ongoing Communication**
    - Maintain regular updates with response teams and management as the situation evolves.

6. Incident Reporting Form (Sample Fields)

Date/Time	Location	Reporter Name	Description	Initial Actions Taken	Notified Persons

YYYY-MM-DD HH:MM	Building/Floor/Area	Full Name	Summary of incident	Brief overview	Who was notified

> **Note:** Always prioritize personal safety and the safety of others. Never attempt containment measures beyond your level of training or authorization.

7. References

- Company Emergency Procedures Manual
- Incident Reporting and Investigation Policy
- IT Security Incident Response Plan (if applicable)

8. Revision History

Version	Date	Description	Author
1.0	2024-06-10	Initial SOP release	SOP Team