

Incident & Accident Investigation Policy

Version: 1.6

Effective Date: 1st June, 2025

Approved by: Anirudh Loya, CEO

Next Review: 1st June, 2026

1. Purpose

The purpose of this policy is to establish a structured approach for investigating and addressing workplace accidents and IT security incidents at **Vrinda Techapps**. This ensures the safety of employees, protection of business operations, and compliance with regulatory requirements.

2. Scope

This policy applies to all employees, contractors, and stakeholders involved in **physical workplace accidents** and **IT-related incidents**, including cybersecurity breaches, data leaks, and system failures.

3. Incident Categories

- **Workplace Accidents:** Injuries, slips, falls, fire hazards, or ergonomic issues.
- **Cybersecurity Incidents:** Data breaches, malware attacks, unauthorized access, and system compromises.
- **Operational Incidents:** IT failures, service disruptions, or compliance violations.

4. Reporting Process

1. **Immediate Response:** Ensure the safety of affected individuals and mitigate damage.
2. **Incident Notification:** Employees must report any incident immediately to their supervisor or the designated **Incident Response Team (IRT)**.
3. **Incident Logging:** The incident must be recorded in the **Incident Register** with details of:
 - Date & Time
 - Location/System affected
 - Description of the incident
 - Initial impact assessment

5. Investigation Process

5.1 Preliminary Investigation

- Assess the severity of the incident.

- Collect initial evidence (system logs, witness statements, CCTV footage, etc.).
- If necessary, escalate to senior management

5.2 Root Cause Analysis (RCA)

Methods used to determine the root cause include:

- **5 Why's Analysis** (Identifying underlying issues through iterative questioning).
- **Fishbone Diagram** (Categorizing potential causes related to People, Process, Technology, and Environment).
- **Forensic IT Investigation** (For cybersecurity-related incidents).

5.3 Corrective & Preventive Actions (CAPA)

- Implement immediate fixes (patching vulnerabilities, first aid, equipment repair, etc.).
- Develop long-term preventive strategies (policy updates, employee training, system hardening, etc.).
- Conduct post-incident reviews and integrate learnings into company policies.

6. Communication & Documentation

- Findings must be **documented** in an **Incident Report** with recommendations for improvement.
- If required, notify **regulatory bodies, clients, and affected parties** in compliance with industry standards.
- Maintain a centralized **Incident Register** for tracking and audits.

7. Review & Continuous Improvement

- Conduct **regular audits and reviews** of the investigation process.
- Organize **awareness training sessions** for employees to prevent future incidents.
- Update policies based on lessons learned from past incidents.

8. Compliance & Responsibilities

- **Employees:** Must report incidents promptly and cooperate during investigations.
- **Incident Response Team (IRT):** Responsible for leading investigations and implementing corrective actions.
- **Management:** Ensures compliance, resources allocation, and enforcement of preventive measures.

Policy Owner: Vrinda Techapps India Pvt Ltd