📝 Incident Response Policy

Version: 1.0
Effective Date: April 2025

Purpose

To provide a standardized process for identifying, reporting, and managing information security incidents.

Scope

Applies to all personnel, including contractors and third parties, who use or access company systems or data.

Definitions

Security Incident: Any event that compromises, or could compromise, the confidentiality, integrity, or availability of information or systems.

Policy

- All suspected incidents must be reported immediately via email or help desk ticket.
- Users must not delete evidence or attempt to contain incidents independently.
- Incident reporting must include:
    - Date/time of detection
    - Systems affected
    - Description of event or symptoms

Response Lifecycle

1. **Identification** – Confirm and assess the incident
2. **Containment** – Limit spread and impact
3. **Eradication** – Remove threat from the environment
4. **Recovery** – Restore systems and operations
5. **Lessons Learned** – Post-mortem review and policy updates

User Responsibilities

- Participate in annual incident response training
- Follow containment directions promptly
- Cooperate fully with security team investigations

Enforcement

Negligent or willful failure to report may result in disciplinary action.