# Incident Response Policy Template

## Purpose

This policy establishes guidelines for responding to cybersecurity incidents that affect the confidentiality, integrity, or availability of systems or data.

## Scope

Applies to all systems, networks, personnel, and vendors interacting with the organization’s IT infrastructure.

## Policy

All incidents must be reported within 1 hour of discovery to the cybersecurity point of contact.

An incident response team (IRT) must be assembled within 4 hours of confirmed incidents.

All incidents must be logged, classified, and reviewed for lessons learned.

Post-incident reviews shall be completed within 7 business days.

## Roles and Responsibilities

IRT Lead: Coordinate investigation and recovery efforts.

IT Team: Support containment, eradication, and recovery activities.

Compliance Officer: Ensure documentation aligns with regulatory requirements.