INCIDENT RESPONSE PLAN

COMPANY NAME:

DATE CREATED:

SCOPE (WHICH DEPARTMENTS ARE INVOLVED?)

AUTHORITY (WHO IS IN CHARGE DURING AN INCIDENT?)

ROLES & RESPONSIBILITIES

Roles	**Responsibilities**
Incident Response Coordinator	
Incident Response Handlers	
Officers	

Created by IT Business Edge

WHAT DEFINES AN INCIDENT FOR THE COMPANY?

WHAT'S THE FIRST THING YOU DO WHEN AN INCIDENT IS DETECTED?

WHAT STEPS DO YOU TAKE TO CONTAIN A THREAT?

INVESTIGATION

During this phase, the incident response team determines the priority, scope, risk, and root cause of the incident.

REMEDIATION

- Identify affected systems and notify affected parties.
- Determine if the incident needs to be reported and which outside parties it needs to be reported to (clients, stakeholders, authorities, etc.)
- Create a post-mortem of the incident to determine which parts of the process were successful or unsuccessful.
- Other steps:

RECOVERY

Analyze the incident for procedural and policy implications. Gather any important metrics and document lessons learned to incorporate into future training and preparation.

ADDITIONAL GUIDELINES (INSIDER THREATS, DEALING WITH LAW ENFORCEMENT, PRIVACY, ETC.)

Created by IT Business Edge