

Incident Management Policy

# Overview/Purpose

Cyber incidents occur frequently. It is important to realize that having an incident response and management policy allows **<Utility Name>** to protect its information, as well as its reputation. This policy requires <**person or group responsible for policy**> to develop the appropriate procedures, reporting, data collection, management responsibility, legal protocols, and communications strategy to allow the staff to successfully understand, manage, and recover from a cyber incident.

This policy defines the requirement for a baseline incident response and management plan to be developed and implemented that will describe the process to investigate a suspected incident, discover an attack and then effectively contain the damage, eradicating the attacker’s presence, and restore the integrity of the network and system.

# Scope

This policy is intended to state the requirement to have an incident response and management plan, along with the phases of incident management, and categories of incidents. It is not intended to specify what goes into the plan or sub-plans.

# Policy

The Incident Response Plan shall:

* Ensure that there is a written incident response plan that includes a definition of personnel roles for handling incidents.   
  The plan shall define the following phases of incident handling:
  + Preparation
  + Detection and Analysis
  + Containment, Eradication and Recovery
  + Post Incident Analysis & Forensics
* Use incident prioritization by determining incident impact:
  + Functional impact – how systems were affected functionality
  + Information impact – what information was accessed
  + Recoverability – how quickly systems can be recovered
  + Define responsibilities during incident response
* Assign job titles and duties for handling computer and network incidents to specific individuals.
* Define management personnel who will support the incident handling process by acting in key decision-making roles.
* Devise organization-wide standards for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.
* Define standards and processes for notifying the appropriate legal and/or regulatory organizations.
* Provide instructions on how to report computer anomalies and incidents. Such information should be included in routine employee awareness training and activities.
* Conduct periodic incident handling drills.
* Review the Plan on a periodic basis.

# Compliance

## Compliance Measurement

The <**person or group responsible for policy**> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by the <**person or group responsible for policy**> in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with **<Utility Name>** HR policies.

# Related Standards, Policies, and Processes

(Cross references to industry standards)

* Adapted from “Cyber Security Policy Framework” (<https://www.nreca.coop/wp-content/uploads/2015/09/cyber_security_policy_framework.docx>)  
  Cyber Security Policy Framework was created by the Kentucky Association of Electric Cooperatives (KAEC) Information Technology (IT) Association - Cyber Security Subcommittee.
* Adapted from “Incident Response and Management” (<http://www.sans.org/critical-security-controls/control/18>)
* Adapted from NIST 800-61r2 – Computer Security Incident Handling Guide  
  (<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>)

# Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible | Accountable | Consulted | Informed |
| IT Manager | **CEO/GM** | **COO**  **CFO** | **All Employees** |

*[Explanatory Note: <Utility Name> should feel free to alter section to reflect the specific responsibility requirement determined by <Utility Name> management.]*

# Approval

\_

<**Insert title of approver**> Date

# Revision History

|  |  |  |
| --- | --- | --- |
| Date of Change(s) | Revised by | Summary of Change(s) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |