

Information Security Incident Response Plan

# Overview/Purpose

The **<Utility Name>** incident response plan defines the preparation for the handling of incidents, and outlines the incident response phases.

# Scope

Proper response to information security incidents requires:

* A designated team with assigned roles
* Internal and external communication lists
* Metrics for determining incident impact
* Testing and response maturing plan
* Defined phases of incident response

*{Some utilities may create SIRT (Security Incident Response Team). The other option is to use ICS (Incident Command System) structure, which several Coops are already using. The advantage of this approach is that the same ICS can be used to handle different types of incidents}*

# Incident Preparation

## Incident Response Team and Roles

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Description | Primary Person | Backup Person |
| Incident Manager | Analyze event information and estimate incident impact. Coordinate Team effort in all phases of response. | IT Manager | IT Administrator |
| Incident Response Team Member | Reports to Incident Manager | IT Administrator, GIS Technician, | IT Administrator, GIS Technician, E&O technician |
| CEO | Provide management support |  |  |
| Legal Counsel | Provide legal support |  |  |
| External Communication | Communicate with BOD, regulators, media | Public Relations or Marketing |  |
| Logistics | Provide logistic support for longer incidents | Clerical or administrative employees |  |

## Contact List and Tools

(Information Security Response Plan - Forms Examples)

### Internal contact list

Internal contact list shows who should be notified internally in case of an incident.

### External contact list

External contact list shows who should be notified externally in case of an incident.

### Tools

Effective response to incident requires preparing OS images, spare hardware, etc.

## Incident Response Improvements

On quarterly basis, the Incident Response Team should review response to one of the threats listed in risk register or one the scenarios included in document *Incident Examples*.  
The goal of this exercise is to review existing documentation and create more detailed procedures, if needed.

## Table Top Exercises

On annual basis, **<Utility Name>** shouldconduct a Table Top Exercise (TTE) to review Emergency Restoration Plan and Information Security Incident Response Plan.

# Incident Detection and Analysis

All **<Utility Name>** employee shall report suspicious activities related to information technology.

Incident indication may also come from local monitoring systems (SIEM, file integrity monitoring) or from external sources.

Reports should be submitted to the Incident Manager, who will use the *Information Security Incident Response Form****,*** and analyze the incident.

Incident analysis factors:

* Sensitivity classification of involved data: Public, Internal, Sensitive, Confidential or Regulated
* Availability classification of involved data: Supportive, Priority or Critical
* What systems are affected by the incident?
* How many computers are affected by the incident?
* What is potential damage caused by the incident?
* What is the estimated time to recover from the incident?

By using these factors, the Incident Manager can determine incident impact:

* Functional impact – how incident affected systems functionality
* Information impact – what information was accessed, modified, and/or deleted
* Recoverability – how quickly systems can be recovered

Since during incident some information technology systems might be not available, this procedure and form should also be kept on mobile devices and as paper copy as well.

*{The impact level of incident can be aligned with RUS Emergency Restoration Plan which uses the following levels: Catastrophic, Critical, Marginal, Insignificant or Remote}*

**Functional Impact Categories**

|  |  |  |
| --- | --- | --- |
| **Category** | **Definition** | **Examples** |
| None | No effect to the organization’s ability to provide all services to all users | * Single computer affected by virus |
| Low | Minimal effect; the organization can still provide all critical services to all users but has lost efficiency | * Two workstations affected by ransomware * Several laptops were affected by virus |
| Medium | Organization has lost the ability to provide a critical service to a subset of system users | * GIS server affected by exploit, maps not updated * AVL affected by DDoS, vehicle locations not updated |
| High | Organization is no longer able to provide some critical services to any users | * OMS and AMI affected by APT * Firewall firmware was changed affecting communication with the Internet |

**Information Impact Categories**

|  |  |  |
| --- | --- | --- |
| **Category** | **Definition** | **Examples** |
| None | No information was exfiltrated, changed, deleted, or otherwise compromised | * Single computer affected by virus |
| Privacy Breach | Sensitive personally identifiable information (PII) of Members or employees was accessed or exfiltrated | * Employees (PII) data was extracted and found on dark web |
| Proprietary Breach | Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated | * Diagrams of fiber communication and substations was accessed from IP address in Iran |
| Integrity Loss | Sensitive or proprietary information was changed or deleted | * Documentation with distribution lines protection settings were changed |

**Recoverability Effort Categories**

|  |  |  |
| --- | --- | --- |
| **Category** | **Definition** | **Examples** |
| Regular | Time to recovery is predictable with existing resources, and will meet RTO | * Affected workstations will be restored in 4 hours |
| Supplemented | Time to recovery is predictable with additional resources and, will exceed RTO | * Restoring systems affected by ransomware require systems and application images |
| Extended | Time to recovery is unpredictable; additional resources and outside help are needed | * Repeated DDoS require ISP support and changing DNS pointers * Software vendor assistance is require in restoring OMS |
| Not Recoverable | Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation | * Member’s PII information published by hackers |

# Containment, Eradication and Recovery

## Containment

The goal of the containment phase is to regain control by limiting the extent of the damage:

* Consider isolating the compromised system(s)
* Analyze business impact of isolating the compromised system(s)
* Prepare for isolation
* Perform isolation and make system backup, if possible

## Eradication

The goal of eradication phase is removing elements of the threat from the systems and networks:

* Consider reloading operating systems and applications
* Applying latest patches
* Disabling unnecessary services
* Consider activating additional monitoring features
* Validating completion of eradication phase

## Recovery

The goal of recovery phase is to return all systems to original functionality:  
*{Some Coops may use Emergency Recovery Plan for recovering specific systems such as phone switch, Outage Management System, UPN, GIS, etc.}*

* Consider restoring system(s) from latest pre-incident backup
* Estimate data loss and verify RPO
* Prepare plan for handling data loss (credit card transaction, outage information, AMI readings, emails)

# Post Incident Analysis & Forensic

The objective of a post incident analysis is to perform a detailed investigation of the incident, to devise approaches for prevention of similar incidents in the future.  
  
Consider using the following options:

|  |  |  |  |
| --- | --- | --- | --- |
|  | In-house | Law enforcement | Forensics Company |
| Cost | Least expensive | Expensive | Most expensive |
| Response Time | Quick | Might be not available, could cause slow response time | Quick response time |
| Skills of investigators | May not have the relevant skills | Dependent on the local law enforcement | Skilled staff |
| Preservation of evidence | Does not ensure evidence integrity | Preserve evidence integrity, acceptable in court | Preserve evidence integrity, acceptable in court |
| Reputation impact | Minimal impact | Potential loss of reputation if certain incident reach the public | Potential loss of reputation if certain incident reach the public |

# Related Standards, Policies, and Processes

* PCI DSS Requirements   
  (<https://www.pcisecuritystandards.org/document_library>)
* 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** | **IT Department** |  |

*[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) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |