Security Incident Management and Breach Response Policy

Table of Contents

What is Incident Management?

Incident management is the process used to assist efforts in identifying, documenting and resolving events (incidents) that impact business operations and its users. The objective is to restore service as quickly as possible, through a fix or temporary resolution.

What is an Incident?

- A breach, attempted breach or other unauthorized access to the production environment
- Any Denial of Service (DoS or DDOS) attack
- Any failure in network infrastructure resources that disrupts services
- Outage – ISP or power failure
- Corrupted database

Policy Statement

This policy describes and defines the methods for identifying, assessing, tracking and responding to security incidents that will impact the business operations at Atlantic Pacific Processing Systems (APPS). Management will provide guidance and direct activities to resolve all incidents. These incidents will be categorized by type and prioritized to meet the business need. To meet and effectively address any incidents, the following principles shall be in-place.

Response Process

- If an incident occurs, APPS personnel will follow the approved process and for each event log, investigate and communicate to management. If necessary, will follow the "escalation" procedure established based on criticality and need.

Security Incident Reporting and Breach Notification Protocol

- All incidents may be logged in the support tool and tracked through to completion. IT and Operations will be responsible for communicating these incidents (depending on their nature) to Management and provide status updates for the duration of the incident. Management will determine if a formal response is needed to any or all customers impacted.

Vendor-related Incidents and Escalation

- In the event a security incident is vendor specific (Datacenter or Processor), APPS will monitor and assess to determine the most appropriate response.

Breach Notification Protocol

1. Internal Notifications
    - If it is determined after investigation that a security breach involving notice-triggering information has occurred, the designated member of Incident Response Team (IRT) shall notify the Management team.

2. External Notification
    - Subsequently, the Management team will determine if notifications (formal responses) are needed to any customers impacted by the event.

Events & Security Breaches
An **event** is any observable occurrence in a system or network such as opening a file or sending an email. An **adverse event** is an event with a negative consequence such as a virus infecting a computer, a system crash, the loss of data, or the unauthorized access to a system or information. **An adverse event that results in, or has the potential to cause, the loss of information confidentiality, availability, or integrity is classified as a security incident.**

Common categories of incidents are malicious code attacks, unauthorized access to systems, denial of services attacks (DOS), and improper use of systems.

Incidents have been categorized into three severity levels based on the potential impact to APPS. The primary role of the IRT is to respond to high-level severity incidents. APPS IT Services will be the primary responder to low and medium level severity incidents.

When classifying severity levels consider the following factors:

- ✓ Has Personally Identifiable Information (PII) of employees been compromised?
- ✓ Have laws or regulations been violated?
- ✓ Has customer data been compromised?
- ✓ Has any APPS corporate information been compromised?
- ✓ What is the potential financial or brand impact to APPS?

Incident Severity Level	Description
Level/Severity 1 - Low	Detection of an event that has minimal impact to systems and services. Examples include SPAM and localized contained malware infections.
Level/Severity 2 - Medium	Incidents that result in isolated loss of system availability or data integrity. Examples include: system crashes, brief outages, and an inadvertent loss or deletion of records.
Level/Severity 3 - High	Incidents that result in, or have the potential to cause, significant impact to the confidentially, availability, or integrity of APPS information. Examples include the compromise of PII information, corporate or customer information, violations of law, and long-term system outages that may cause significant impact to APPS or its customers.

Purpose

The purpose of this Incident Management and Breach Response Policy is to ensure:

- A well-planned response procedure is in-place;
- Security incidents are communicated quickly;
- Corrective actions are timely implemented;
- The integrity and confidentiality of information is intact;
- Loss of service is prevented or mitigated; and
- Compliance with legal requirements.

Responsibility & Scope

The Chief Information Officer has the primary responsibility for the implementation and monitoring of this incident policy, its standards and any good practices.

This Incident Management and Breach Response Policy will apply to:

- All infrastructure, electronic communication systems, networks and other IT assets used in support of business operations and hosting of the core service(s) and information on and for customers.

Non-incidents that WILL NOT apply include:

- Routine detection and remediation of a localized “virus,” “malware” or similar issues.

Response Plan, Process Flow, Checklist and Key Requirements

Upon determination that a formal response is required, the following actions will be used to bring the incident to resolution:

Detection

- a. Document the Incident
- b. Communicate incident as needed internally - immediately

Coordination

1. Ensure the Security Officer has been notified by:
    - a. Sending an email if possible to security@approcessing.com requesting acknowledgement of the potential incident.
    - b. Call the Security Officer to receive verbal confirmation that the incident has been acknowledged.
2. If computer systems are involved, isolate the affected system(s) by:
    - a. Disconnecting the network cable from the device
    - b. DO NOT disconnect power from the device or turn the device off

Mitigation and Containment

1. The immediate primary goal is to halt any potential security issue that may have occurred. This must be done with a minimum interruption to the operation of the business and the affected systems.
2. For computer systems:
    - a. Ensure step 2 under Coordination above has been completed.
    - b. Verify that logical access is no longer possible without direct access to the workstation
3. For physical access systems:
    - a. Verify physical access is restricted to only those with an immediate need to access the affected systems for forensic purposes.

Initial Forensic Analysis

1. The Security Officer shall begin analysis by determining what data may have been compromised.
2. As soon as personnel information or APPS proprietary information is suspected of being compromised the Security Officer shall immediately notify the corporate executives to determine the appropriate next course of action.
3. The Security Officer shall perform no additional analysis of the systems until the executive management has determined the appropriate course of action.

Responsibility and Execution of Response Plan

The designated Security Officer is responsible for coordinating communication among members of the Incident Response Team. Each member of the Incident Response Team is responsible for communicating potential incidents to the Security Officer as quickly as possible.

- a. If compromised, after containment, meet with the executive team to understand the extent of the incident/breach, what credit card or personal information was viewed or taken and the subsequent reporting to external parties of this breach.
    - i. Check required customer/authorities response actions needed
- b. Finalize handling and provide **Incident Closure Report with final analysis.**

Incident Response Team Members

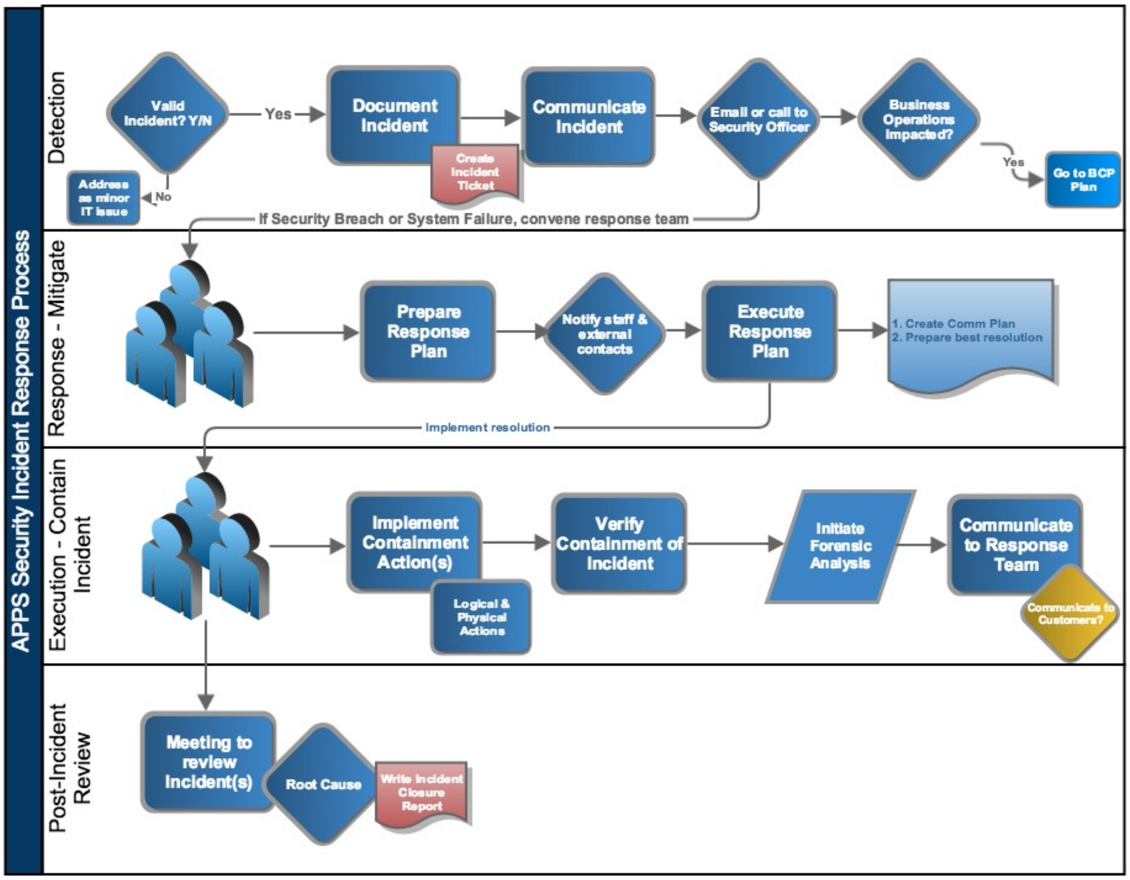
- Security Officer
- VP of Operations
- CIO
- Head of HR (if incident related to employee data)

Note: An incident response may range from getting a critical system back online, gathering evidence, taking appropriate legal action against individual(s), or in some cases notifying appropriate third parties of inappropriate activity originating from their network.

Key Requirements:

1. Perform annual testing of Incident Response Plan
2. Include training of key members
3. Incident or Emergency Response team will be available 24/7 to meet key obligations

Workflow


APPS Security Incident Response Process
Detection
Valid Incident? Y/N
Yes
Document Incident
Create Incident Ticket
Communicate Incident
Email or call to Security Officer
Business Operations Impacted?
Yes
Go to BCP Plan
No
Address as minor IT issue
If Security Breach or System Failure, convene response team
Response - Mitigate
Prepare Response Plan
Notify staff & external contacts
Execute Response Plan
1. Create Comm Plan
2. Prepare best resolution
Implement resolution
Execution - Contain Incident
Implement Containment Action(s)
Logical & Physical Actions
Verify Containment of Incident
Initiate Forensic Analysis
Communicate to Response Team
Communicate to Customers?
Post-Incident Review
Meeting to review Incident(s)
Root Cause
Write Incident Closure Report

Who Should Read and Understand This Policy

This policy should be read by:

Management and all **APPS** personnel:

- To ensure that security measurements are updated and taken seriously.
- To ensure protective measures are consistently implemented and followed.
- To be aware of and prepared for security issues and risks that may arise.

Enforcement & Exceptions

APPS reserves the right to temporarily or permanently suspend, block, or restrict access to information assets when is reasonably appears necessary to do so to protect the confidentiality, integrity, availability, or functionality of those assets.

If it is determined that there is non-compliance with or a violation of this policy, the employee(s) or contracted individual(s) may be subject to immediate disciplinary action, up to and including termination.

Policy Management

This policy will be reviewed, at least annually, by the author or designee and updated as necessary to properly address current business needs.

References

- Information, Confidentiality & Cyber-security Policy
- Security Standards
- SOC Reports from **APPS** Datacenters

Appendix - Definitions

- Security Incident - A Security Incident (Incident) is described as one or more of the following conditions:
  - Any potential violation of Federal/State law, regulation, or APPS policy involving an Infrastructure Production asset
  - A breach, attempted breach or other unauthorized access to the production environment
  - Any Denial of Service (DoS or DDOS) attack or related incident
  - Any failure in network or computer systems that disrupts APPS

- Incident Response Team – A team of individuals formed before or in response to a Security Incident.

- Security Breach
  - An unauthorized acquisition of data that compromises the security, confidentiality or integrity of information maintained by APPS.