[Insert Company Name and Logo]	
Title: Security Incident Response	**P&P #:**
Approval Date:	**Review:**
Effective Date:	**Security Team**

Purpose: This policy is designed to protect the organizational resources against intrusion. The Security Incident Response Plan defines what constitutes a security incident and outlines the incident response phases.

Scope: This policy applies to all employees and other workforce members (whether paid, volunteer or contractor) having access to the organization's information systems and/or network in any facility under the organization's ownership.

Policy:

1. Incident Response Goals:
   a. Verify that an incident occurred
   b. Maintain or Restore Business Continuity
   c. Reduce the incident impact
   d. Determine how the attack was perpetrated or how the incident happened
   e. Prevent future attacks or incidents
   f. Improve security and incident response
   g. Prosecute illegal activity
   h. Keep management informed of the situation and response
2. Incident Definition
   a. An incident is any one or more of the following:
      i. Loss of information confidentiality (data theft)
      ii. Compromise of information integrity (damage to data or unauthorized modification)
      iii. Theft of physical IT asset including computers, storage devices, printers, etc.
      iv. Damage to physical IT assets including computers, storage devices, printers, etc.
      v. Denial of service
      vi. Misuse of services, information, or assets
      vii. Infection of systems by unauthorized or hostile software
      viii. An attempt at unauthorized access
      ix. Unauthorized changes to organizational hardware, software, or configuration
      x. Reports of unusual system behavior
      xi. Responses to intrusion detection alarms
3. Roles and Responsibilities

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

a. The incident managers responsible for managing the response to a security incident include:

i. The Security Officer

ii. The Privacy Officer

iii. The IT Manager (if applicable)

iv. The Security Incident Response Team (if applicable)

4. Implementing Procedures

a. Reporting Security incidents

i. Any member of [Company name] who suspects the occurrence of a security incident must report incidents through the following channels:

1. All suspected high severity events as defined below, including those involving possible breaches of secured and regulated data, must be reported directly to one of the incident response managers listed previously.

2. All other suspected incidents must also be reported to an incident response manager.

a. These incidents may be first reported to departmental IT support personnel.

b. Security Incident Levels of Severity

i. Incident response will be managed based on the level of severity of the incident.

ii. The level of severity is a measure of its impact on, or threat to, the operation or integrity of the institution and its information.

iii. It determines the priority for handling the incident, who manages the incident, and the timing and extent of the response.

iv. Three levels of incident severity will be used to guide incident response: high, medium, and low.

1. The severity of a security incident will be considered "high " if any of the following conditions exist:

a. Threatens to have a significant adverse impact on many systems and/or people (for example, the entire institution is affected)

b. Poses a potential large financial risk or legal liability to [Insert Company Name]

c. Threatens confidential data (for example, the compromise of a server that contains names with social security numbers or credit card information)

d. Adversely impacts an enterprise system or service critical to the operation of a major portion of [Company Name] (for example, e-mail, financial information system, human resources information system, or Internet service)

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

e. Poses a significant and immediate threat to human safety, such as a death-threat to an individual or group

f. Has a high probability of propagating to many other systems, causing significant damage or disruption

2. The severity of a security incident will be considered "medium" if any of the following conditions exist:
   a. Adversely impacts a moderate number of systems and/or people, such as an individual department, unit, or building
   b. Adversely impacts a non-critical enterprise system or service
   c. Adversely impacts a departmental system or service, such as a departmental file server
   d. Disrupts a building or departmental network
   e. Has a moderate probability of propagating to other systems, causing moderate damage or disruption
3. Low severity incidents have the following characteristics:
   a. Adversely impacts a very small number of systems or individuals
   b. Disrupts a very small number of network devices or segments
   c. Has little or no risk of propagation or causes only minimal disruption or damage in their attempt to propagate

Violations:
Any user found to have violated this policy may be subject to disciplinary action, up to an including termination of employment.
In addition, [Insert Company Name] may report the matter to civil and/or criminal authorities as may be required by law.

Attachments: None

Related Policies

None

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.