HealthLX Security Incident Response Plan

Last Updated: 2/01/2025

Table of contents

Overview

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.

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 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 assets 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
    a. The incident managers responsible for managing the response to a security incident include:
        i. The Security Officer
        ii. The IT Manager (if applicable)
        iii. The management team

4. Implementing Procedures
    a. Reporting Security incidents
        i. Any member of HealthLX 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 protected health information (PHI), 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 a large number of systems and/or people (for example, the entire institution is affected)
                b. Poses a potential large financial risk or legal liability to HealthLX
                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 HealthLX (for example, e-mail, financial information system, human resources information system, or Internet service)
                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

c. Incident Response
    i. The following summarizes the handling of IT security incidents based on incident severity, including response time, the responsible incident managers, and notification and reporting requirements.
        1. High Severity
            a. Immediate response, report to anyone indicated for Incident Response.
            b. If breach of PHI, see Breach Notification Procedures for additional notification requirements.
            c. Create an Incident Response Report describing the whole event.
        2. Medium Severity
            a. Respond within 4 hours, report to anyone indicated for Incident Response.
            b. If breach of PHI, see Breach Notification Procedures for additional notification requirements.
            c. Create an Incident Response Report only if a Breach occurred, or one is requested by the Security Officer.
        3. Low Severity
            a. Respond within 24 hours, report to the IT manager or team.
            b. Create an Incident Response Report only if a Breach occurred, or one is requested by the Security Officer.
    ii. Should there be a Breach of PHI, the Security Officer will follow the Breach Notification steps.
    iii. After the incident has been handled, the Incident Response Team or Manager should determine if changes need to be made to prevent a similar incident from happening.

Violations:

1. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
2. Violation may also result in civil and criminal penalties to HealthLX as determined by federal and state laws and regulations related to loss of data.