Incident Response Policy

1.0 Overview

In order to reduce exposure to our user information and other confidential information, we have developed this policy as a means to define the appropriate actions to take should any of the company's systems be compromised.

2.0 Purpose

In the unlikely event that a security breach occurs, "Company Name"s staff will escalate all known information to the appropriate managers. In addition, staff are authorized to take any immediate and appropriate actions to ensure no further damage is sustained. For examples of possible security incidents please click here. Any questions or comments about this policy should be directed to Information Systems.

3.0 Scope

This policy applies to all systems, networks, and data within the company's operating environment.

4.0 Policy

Immediately following the detection of a breach of security, the Chief Information Officer and the Information Security Officer must be notified. All issues must be documented on the Incident Reporting Form and supplied to the Information Security Officer following the incident. Secure mechanisms should be used for all communications regarding the breach. Use communications that do not involve the compromised system or network. Do not send email from compromised systems or networks. Upstream sites (sites that were involved in an intrusion prior to the system becoming involved) and downstream sites (sites that were involved after the site experienced an intrusion) need to be informed of the attacks as well. The Information Security Officer will ensure that all other organizations are informed about the involvement of their systems so they too can take necessary steps to respond to an intrusion. The Information Security Officer must ensure that an accurate, detailed log of all contacts and the information exchanged is maintained. Information pertaining to a security breach will only be released by the CEO, President or Vice President of the Company.

5.0 Enforcement

Anyone found to have violated this policy may be subject to disciplinary action, up to and including suspension of access to technology resources or termination of employment. Clients, patients, and or staff may be referred to HR for discipline. A violation of this policy by a temporary worker, contractor or vendor may result in action up to and including termination of their contract or assignment with "Company Name"s.