Incident Reporting Procedure

1.0 Overview

This procedure will ensure that “Company Name”s Information Security staff is properly informed of any information security incident.

2.0 Purpose

The purpose of this procedure is to provide all “Company Name”s personnel the appropriate information to report any information security incident.

3.0 Scope

This procedure addresses all “Company Name”s information technology resources.

4.0 Procedure

4.1 Incident Identification

Information security incidents can be interpreted differently by multiple people. To help define what security incidents need to be reported, the following list shows a few examples of what should be reported.

- Virus/malware on a production server
- Compromised account (email, active directory, LOB, etc.)
- Stolen property that contains Company data
- Strange network activity
- Major violation of one of the Information Technology Policies.

This list is by no means complete, but simply a guideline. If there is ever a doubt of whether or not to report an incident, you can contact the Information Security Officer for more information.

4.2 Incident Report

Once the incident has been identified, alert the Information Security Officer via phone. Then fill out the Incident Response Form and send it to the Information Security Officer via email or fax. Proper responses to incidents often depend on timely action, requiring all incidents be reported as soon as possible. Incidents must be reported within 24 hours of identification.

4.3 Incident Resolution

Once the Information Security Officer receives the Incident Response Form, he/she will evaluate what steps need to occur next. Depending on the severity of the situation, an Incident Response Team (IRT) may be deployed to look into the situation further, or the incident may merely be documented by Information Security personnel and taken care of by the local technicians.

5.0 Definitions

Incident Response Team (IRT)

A group of people who prepare for and respond to any emergency incident. The team will vary depending on the particular type of incident.

6.0 Revision History