# Incident Response Plan

### 1 Introduction & Overview

This document outlines the specifics for the company Incident Response Plan. It contains instructions and guidelines on how to handle security related issues when they arrive. Employees should be aware of the following procedures and act appropriately if and when a security incident occurs.

## 2 Incident Response Procedures

Incident response is broken down into five (5) main categories which include the following:

* Preparing for an incident
  + Detecting an incident
* Responding to and containing an incident
* Recovery from an incident
* Post-incident activities and awareness

### 3 Preparing for an Incident

All employees should be aware of common security threats and computer incidents that may potentially compromise the organization’s network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization as a whole. This plan should be viewed as a set of procedures for examining a computer security incident. There are numerous security threats and computer incidents that are potentially detrimental to any organization, such as the following:

* Malicious or careless employees
* Malware (computer virus, worm, Trojan horse, rootkit, spyware, etc.)
* Social engineering
* Spam
* Spoofing and phishing
* Denial of service
* Distributed denial of service
* Man-in-the-middle attacks
* Additional network attacks, including hacking and other common attack vectors
* Physical and environmental conditions resulting in threats to the organization’s system resources

3.1 Adequately preparing for an incident requires security personnel to be aware of common threats to systems and to implement safeguards and control mechanisms that protect system resources within the company. Testing the IR plan is done annually (see *Incident Response Test and Exercise Procedure).*

3.2 A vital component of preparing for an incident is ensuring that all personnel have relevant security training pertinent to their roles and responsibilities. Additionally, all system components and other IT resources deemed critical must be securely hardened with best of breed hardening and configurations standards at all times. Sources used may include, but are not limited to the following:

* NIST (<http://www.nist.gov>)
* SANS ([http://www.sans.org](http://www.sans.org/))
* CERT ([http://www.cisecurity.org](http://www.cisecurity.org/))
* ISACA ([http://www.isaca.org](http://www.isaca.org/))
* BITS & Shared Assessments ([http://www.sharedassessments.org](http://www.sharedassessments.org/))

3.3 The numerous policies and procedures outlined within the *PCI Information Security Policy* document serve as an excellent resource for ensuring adequate safeguards are in place for these very systems and critical IT resources. Specifically, the Security Awareness Training initiatives provide excellent resources that allow employees to keep abreast of significant threats to company assets.

3.4 Moreover, an Incident Response Team is to have clear roles and responsibilities for properly responding to any incident. Members of the team are to be available 24/7 for incident response. Preparation is just as important as the response to the incident. Other aspects of preparing for an incident include the necessary steps, processes and procedures to take once an incident has occurred. This also includes an understanding of what actions are to be taken with respective third parties, if necessary, such as clients, law enforcement agencies, local/federal/state agencies, if necessary; as well as the media and any other third parties considered to be in scope.

### 4 Detecting an Incident

Detecting an incident requires a true commitment by all employees to be constantly aware of their surroundings for any type of social engineering, physical or environmental threat. Additionally, detection also requires due diligence and consistency by authorized employees regarding the secure configuration and review of network and system logs, being aware of network traffic anomalies and any suspicious or disruptive network patterns or incidents. Employees responsible for reviewing network and system logs (firewalls, routers, switches, IDS/IPS, operating systems, applications, databases, etc.) are, as a result of these reviews, to report any malicious, suspicious or disruptive event immediately to the Incident Response Team.

4.1 The Incident Response Team can only respond to a given incident if they are made aware of the issue. Detection, therefore, is a vital component of the Incident Response Plan. Accordingly, all system components and additional IT resources deemed critical are to be inventoried in a manner that describes the naming convention of the device, the use of the device, who has system administrative rights of these devices, which logging and audit trail mechanisms are in place and who reviews these logging and audit trails on a consistent basis.

### 5 Responding to and Containing an Incident

Any incident deemed to be a relevant threat to the organization requires a rapid response from authorized personnel, such as the Incident Response Team. This rapid response will follow a standard course of action designed to minimize the impact of the incident to the organization’s critical network and system infrastructure.

The following documented response mechanisms serve as the Standard Operating Procedures (SOP) for responding to any incident within the organization:

1. For any incident that has been detected, the Incident Response Team is to be immediately notified. Members of the team and their duties are contained in the *Incident Response Team List.*
2. The Incident Response Team is to formally assume control and to identify the threat and its severity to the organization’s information systems.
3. In identifying the threat, the Incident Response Team is to specifically identify which resources are at risk, both internal and external, and which harmful processes are currently running on resources that have been identified as *at risk*.
4. The Incident Response Team is to make a determination if the resources at risk (hardware, software, etc.) require physical or logical removal. Resources which pose a significant threat to the continuity of the business are to be immediately removed or isolated, either physically or logically.

Resources which may require physical or logical removal or isolation may include, but are not limited to the following:

* All IP addresses in use
* Firewalls, routers, switches, wireless access points
* Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS)
* Any enterprise-wide applications (CRM systems, etc.)
* Remote access
* Point-to-point secure data transmission methods
* Authentication servers (RADIUS)
* Servers (web, proxy, file, email, DNS, etc.)
* Operating systems
* Databases
* Applications

1. If the incident has affected the cardholder data environment in any way and has impacted the system components within this environment, it must be immediately reported to the major payment brands.

Listed below are links to the major payment brands, which also supply information on how to handle an incident that has resulted from a breach of the cardholder data environment. It is the policy of the company to formally acknowledge and adhere to these guidelines as set forth by the major payment brands.

|  |  |
| --- | --- |
| **Payment Brand** | **Information on Incident Handling and Reporting** |
| Visa | <http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html> |
| MasterCard | <http://www.mastercard.com/us/merchant/security/fraud_prevention.html> |
| American Express | <https://www.americanexpress.com/us/content/merchant/fraud-prevention.html> |
| Discover | <http://www.discovernetwork.com/fraudsecurity/databreach.html> |
| JCB | <http://www.jcb-global.com/english/jdsp/index.html> |

1. If the incident has in any way resulted in a criminal matter that may be readily identified, it must be immediately reported to law enforcement officials. This may include, but is not limited to the following:

* Local law enforcement
* The United States Secret Service (for credit card fraud)
* The Federal Bureau of Investigation (FBI)

1. Investigating the incident is also a critical process within the Incident Response plan. Proper investigative techniques are to include, but are not limited to the following:

* Understanding how the incident occurred and what led to the compromise
* Reviewing all necessary system documentation, such as logs, audit trails, rule sets, configuration and hardening standards
* Interviewing personnel
* Examining third party providers and their respective products and services that are utilized within the network architecture
* If warranted, a third party resource for assisting in the investigation of the incident may be utilized (at management’s discretion)

### 6 Recovery from an Incident

Recovery procedures will include, but are not limited to the following:

* Restoring systems from clean backups
* Rebuilding systems as needed and warranted
* Replacing systems as needed
* Reconfiguring network security (stronger, more adaptive configuration and hardening rules) for all system components

The recovery procedures will be commensurate with the incident that has occurred. This will be conducted on a case-by-case basis with all aspects of the recovery process fully documented.

### 7 Post-Incident Activities and Awareness

A formal and documented Incident Response Report is to be compiled and given to management within an acceptable time frame following the incident. The report must contain the following elements:

* Detailed description of the incident
* Response mechanisms undertaken
* Reporting activities to all relevant third parties as needed
* Recovery activities undertaken for restoring affected systems
* A list of Lessons Learned from the incident and which initiative can be taken to mitigate the likelihood of future incidents