**Incident Response Plan Introduction and Commentary**

In accordance with industry ‘best practices’ and to comply with numerous compliance regulations, (your company name here) has implemented various procedures, policies and guidelines in order to protect the confidentiality, integrity and availability (CIA) of their critical client data and their computing resources. This Incident Response Plan is one such procedural document intended to prepare (your company name here) to address security incidents. Regular testing and refinement of this plan will help (your company name here) prepare for adverse security incidents and ultimately help them to manage and minimize risk.

It is anticipated that as new technologies and new requirements are introduced this document will need to be modified and should be reviewed at least annually. This function will be performed by members of the security team at the direction of the Chief Information Security Officer.

 **Incident Response Plan Overview**

There are many different security incidents that can occur with assorted severity levels and not all incidents will require focus on each step. However it is important to be prepared and understand that typically different phases exist in responding to an incident, and the goals and objectives of each phase. The different phases of a security incident response plan at (your company name here) are as follows:

* Prepare
* Identify
* Contain
* Eradicate
* Recover
* Review

**Prepare**

In preparing for security incidents several items need to be addressed.

* Incident handling team should include security officers, system analysts and human resources personnel
* End users and analysts should be trained at an appropriate level. Login banner and warning messages should be posted.
* Contact information is included as an appendix to this document and should be available in hard copy for:
	+ personnel that might assist in handling an incident
	+ key partners who may need to be notified
	+ business owners to make key business decisions
	+ outside support analysts with security expertise
* Backups should be taken and tested!
* Supplies to assist the team in the event of an incident (sometimes referred to a jump bag)
	+ An empty notebook (Thorough documentation should be done throughout an incident to include hand written notes in a fresh notebook.)
	+ Boot CDs to analyze hard drives and recover passwords
	+ Petty cash (food, cabs, batteries as needed)

**Identify**

Awareness that a security incident has occurred can originate from different sources such as technical people, end users or even clients.

Best practices suggests to declare that an incident has occurred when security officers’ sense that an adverse risk to the company exists and then assemble the team and implement the plan. It is also suggested to early on have multiple people involved, to save all key system files or records such as log files and start detailed documentation as soon as possible.

Ultimately business owners need to be involved in many security incidents to decide what are the goals in handling a particular incident, such as immediate business recovery or forensic examination.

**Contain**

Following basic procedures can contain many incidents. Specific procedures will frequently depend on the nature of the incident, as well as the direction of the business owner. Remember that a compromised machine might not present valid data! Basic steps to consider include:

* Obtain and analyze as much system information as possible including key files and possibly a backup of the compromised machine for later forensic analysis.
* Powering off a machine might lose data and evidence. Preferably disconnecting the LAN cable facilitates containment and forensic activity. (Putting the computer on a separate network with a network analyzer might help analyzing network activity)
* If one machine has been exploited others might be vulnerable. Actions that might need to be taken on a large scale might include:
	+ - Download security patches from vendors
		- Update antivirus signatures
		- Close firewall ports
		- Disable compromised accounts
		- Run vulnerability analyzers to see where other vulnerable hosts are
		- Change passwords as appropriate

**Eradicate**

To eradicate the problem specific procedures will frequently depend on the nature of the incident as well as the direction of the business owner. Key considerations include:

* Boot CDs should be used to access data on compromised machines. (Rootkits installed on compromised machines might affect basic system level utilities and discourage use of a compromised host)
* If machines OS has been compromised it needs to be rebuilt using hardened machines on appropriate platforms
* Test any backups prior to restore and monitor for a new incident.
* Document everything.

**Recover**

The recovery phase’s goal is to return safely to production. Once again specific actions might depend on the nature of the incident as well as the direction of the business owner. Key considerations include:

* Retest the system preferably with a variety of end users.
* Consider timing of the return to production.
* Discuss customer notification and their concerns
* Discuss media handling issues
* Continue to monitor for security incidents

**Review**

This phase is to allow (your company name here) to better handle future security incidents. A final report should be written describing the incident and how it was handled using the Incident reporting form. Suggestions for handling future incidents and reworking this document should be included in this report.

**Contact information**

1. Personnel that might assist in handling an incident
2. Key partners who may need to be notified
3. Business owners to make key business decisions
4. Outside support analysts with security expertise

Additional service provider contacts