TO: Philip Carson

FROM: IT Staff

Subject: 056 – Corporate Vulnerability Policy

The information security team’s duty is to ensure the integrity of information/resources, to investigate incidents, to ensure conformance to security policies, or to monitor user/system activity where appropriate.

* To ensure the integrity of information/resources, the information security team must be allowed to scan any files or systems they need to, to search for intrusions into the system, or other things relating to the security needs of the company. Some of the tools (but not all) the team needs to utilize are:
  + Nessus
  + Snort
  + Splunk
  + nmap
  + netstat
  + lsof
* The information security team has the authority to scan with tools like those above regularly and patch anything, or ban any IP-addresses that seem necessary based on suspicious activity.
* The information security team must have the authority to investigate incidents in a reasonable time frame without any unreasonable limitations.
* Any information gathered by the information security team must be kept anonymous and must not be distributed to anyone outside the security team, under any circumstances.
* A privacy policy should be established to ensure the rights of users and employees, but also allows the information security team to do their job.
* The information security team must have support from management to ensure conformance to security policies, such as the password creation policy, social networking policies, server security policies, and the general security policies, among company employees.
* Audits and vulnerability scans are to be performed weekly at minimum, but can be performed continuously if necessary.
* When members of the security team are terminated, all access credentials must be immediately changed to eliminate potential access to the system for that employee.
* All members of the security team should submit to background checks to verify that they are trustworthy individuals.
* The security team should report directly to upper management to ensure that vulnerabilities and incidents are discussed and handled in a fashion that is consistent with the company’s policies and puts the company in the best light possible.

Sincerely,

The IT Staff