TO: Philip Carson

FROM: IT STAFF

Subject: 054 – Corporate Server Security Policy

It is important to secure the servers inside our production network, or used in a production capacity, to reduce the vulnerabilities of our company’s resources. The following rules should be followed to secure production servers:

* Servers should be located in a physically secure environment, meaning all employees accessing the servers will be required to use key access to enter.
* Servers should be located offsite in an approved data center that provides security features such as:
  + No physical windows
  + Controlled access
  + Certified employees that have passed background checks
  + Cameras
  + At least two factor access including passwords and biometrics
* All machines must be logged out of or locked prior to leaving the machine unattended.
* All SSH access should be through an administrative user that is not root (or administrator in Windows).
* All services that are not required for public use, except those such as FTP, HTTP, SSH, should be firewalled.
* All non-required services need to be shutdown, such as cups, rpcdaemons, portmap, avahi-daemon etc.
* All daemon processes should be running on a specific internal interface instead of listening to all external interfaces.
* Administrative passwords follow the password creation policy that you received earlier.
* Administrative passwords should only be available to the IT Department.
* All services should be audited for file based permissions so that they’re not open to the world.
* Anytime any change goes into a system it needs to be documented and there needs to be a Statement of Work or a Method of Procedure that needs to be approved by administration.
* If possible, the firewall should use whitelist policies as opposed to blacklist policies.
* The company should perform security audits to any changes in application code.
* The servers should be backed up fully every week and incrementally every day, on tapes. The tapes should be stored in a different location than the servers.
* Log-files should be read-only for the administrator.
* New users should be approved by administration first.
* Processes should be in place such that terminated employees are removed from the server the day they are terminated.
* Administrator passwords should be changed every month.

These suggestions will improve the security of our company.

Sincerely,

The IT Staff