TO: Philip Carson

FROM: IT Staff

Subject: 050 – Corporate Security Acceptable Use Policy

It is important to define a policy for acceptable use of equipment and computing services in order to not introduce vulnerabilities into our system, and jeopardize our corporate resources and proprietary information.

Computing services and equipment should only be used for work purposes, as we cannot ensure the security of outside applications and tools.

Secure passwords are necessary. Weak passwords represent a rather large door into our business. If someone gets their hands on one of our passwords, whatever they access becomes compromised, and depending on what passwords they have, they can cause a lot of damage. To prevent this, please follow the following guidelines about password creation:

* Use at least 8 letters, containing at least one capital letter, one number, and one symbol excluding the ones in the following list: “ ` ‘ , \ /
* Don’t use common phrases or sentences.
* Don’t use personal information, such as birthdays or pet names. If someone gains access to this information they may be able to guess your password.
* New passwords must be at least 3 characters different from the previous password.
* Always use a different password for each login.

Make sure you never give your password to anyone, not even your boss or IT staff.

Physical security is also important. If you have a laptop that you bring home, make sure that nobody has access to it, don’t leave it unattended, and that its login password follows the requirements above. Also, don’t log in to open wireless networks, such as those at a coffee shop, on your laptop, as such networks are vulnerable. Don’t ever plug in a flash drive that you don’t own, as there may be viruses or other malware on it. At your workstations, always lock your computers, and the IT Staff will implement a policy where when your screen saver comes on, the computer will lock itself.

Only install software that is sanctioned by the IT Staff. If you wish to install additional software, get clearance from IT first.

If you ever suspect or experience a security breach, such as a compromised password or a stolen laptop, please report it to the IT Staff immediately.

If you are unsure of, or have questions about, any part of this policy, please contact us.

Sincerely,

The IT Staff