**SOP – Computer Security and**  ****

**The Threats**

Our biggest threats are:

1. Someone hacking our email system and sending out malicious emails.
2. Someone hacking into customer data.
3. Someone stealing computers.

Never store your LastPass master password on your computer, and if you need to write it down temporarily to learn it, destroy it as soon as you can. Never give it to ANYONE else!

**Team Computers**

We are using LastPass password protection for all Team passwords to make it more difficult to hack into. Essentially, the only way a hacker will be able to hack into our systems is if they find our LastPass password OR we leave the computer running with LastPass open and someone gets on our computers in person.

Therefore, the biggest concern is protecting LastPass! When we close up shop for the evening, we should sign out of Last Pass. That way if someone steals a computer overnight, they will only get the info on the computer itself, not any of our online storage or emails. Re-signing in daily will help to remember the long LastPass passwords too!

Rules for Team and personal computers with Team info on them:

1. Always secure to desks overnight in the office – Use computer locks.
2. Normally sign out of everything and shut down overnight. Includes LastPass. May leave running if updating something, but sign out of LastPass.
3. Lock inner office door.

**Multi-Factor Authentication**

Multi-Factor Authentication means having to use another device to prove you are you when signing in. It’s the best security out there right now! A hacker has to hack your computer and your cell phone at the same time to get in.

We will use multi-factor authentication with these specific sites which pose the most risk in being hacked:

* LastPass master sign in (your sign in)
* Outlook and all email sites
* MS Office 365
* DropBox

(You should set up your personal bank and email accounts with multi-factor authentication also.)

You can set your computer as a “Trusted Computer” on many sites and avoid the multi-factor authentication unless you’re trying to sign in from another untrusted computer.

Each of the users should set their Last Pass Extension Security with the two below shown numbers. You can experiment with the Auto Log out after idle minutes if needed. These preferences can be found on Chrome by:

* Click on LastPass red square icon in upper right ribbon
* Click on Preferences
* Set values and SAVE.



ALWAYS log off of your computer if you are going to be away from it for more than a few minutes in the office. Log off by: [Windows Key] + “L”

Log out of LastPass anytime you’re leaving for a longer time or overnight.

**Team and Personal Computers at Home**

If leaving a computer unattended at home, please log out of LastPass and Outlook before you go. You only have to re-log in one time for each when you return. Not that difficult!

If a computer is compromised or stolen (even if you aren’t sure), please call and text Tom immediately. He can shut down your LastPass account temporarily without much trouble to re-establish it once we find it. Much better to be safe than sorry!

**Personal Computers and Mobile Devices**

In order to use Team Outlook and LastPass on your personal computer, you must have a windows password for protection (signing in to the computer). If using LastPass on your personal or a foreign computer, ALWAYS log completely out of LastPass at the end of each session. That is extremely important! And only use LastPass to log into our email system on foreign computers for more security. If your personal computer is stolen or misplaced, let me know too and we’ll sign you out immediately from the LastPass website and issue you a new password. It’s that easy.

**Wifi**

NEVER use a wifi with a computer or cellular device that has ANY Team data on it, that includes your personal devices, unless that wifi is password protected and private. That means NEVER use a coffee shop or hotel wifi, or any other organization’s wifi. And your home system must have a tough to crack password. If kids outside your household have the password, then don’t use if for business. Personal hot spots on your cell phone are secure and the best to use when outside normal secure areas (like in a hotel).

**Password Strengths**

You will only need to use this once each time you start up your computer!

You can also access LastPass from foreign computers, BUT BE SURE TO LOG OUT!

12 characters min, non-words, some caps, some numbers, some symbols

TE must approve first, do not store on computers, prefer head only

Change every 6 months to year

EXAMPLES – These are very tough for the auto-hackers to break:

Iesfb7dawatagr8t!

I eat sticks for breakfast 7 days a week and they are gr8t!

MNia#t10cahaCVT?

My Nissan is a #twenty 10 car and has a Constant Velocity Transmission?

OosiPALat’rgr8t!

Our office staff includes Peggy, Annette and Lexi and they’re gr8t!

XP#b$6pakLR&

Hard to remember!