CYBERSECURITY GUIDE

PASSWORDS	• NEVER use the same password twice
	• ALWAYS setup MFA (Multi-Factor Authentication)
	• Use a minimum of 16 characters
	• Include a combination of:
	  ○ Uppercase
	  ○ Lowercase
	  ○ Numbers
	  ○ Symbols
	• DO NOT USE:
	  ○ Your username
	  ○ Your name, kids name, phone number, address, social security number, names of family members, or your pets name
	  ○ Common words like “password” or “123”
	  ○ Do not use words that can be found in the dictionary. If you must use dictionary words, try adding a numeral to them, as well as punctuation at the beginning or end of the word (or both!).

PASSWORD MANAGER	• USE a password manager so you can maintain and manage complex passwords
	• Some popular password managers:
	  ○ LastPass (free version available)- www.lastpass.com
	  ○ DashLane- www.dashlane.com
	  ○ 1Password- www.1password.com
	• DO NOT use google save your password feature

PHISHING EMAILS	• REMEMBER to mouse over/hover on any links in emails to verify if legitimate • ONLY click on links from known sources • TRUST YOUR GUT, if you question an email, contact the sender by phone to verify • CHECK sender email address is one you recognize, be aware of impersonation • DO NOT forward phishing emails, DELETE phishing emails

TELLTALE SIGNS YOU HAVE BEEN HACKED	• NO NEW EMAILS for hours • ANTI VIRUS is turned off or uninstalled • POP-UPS and REDIRECTIONS to other websites • SLOW COMPUTER and a lot of computer activity when you are not using it • IF YOU THINK YOU HAVE BEEN HACKED TURN OFF YOUR COMPUTER AND ENGAGE AN IT PROFESSIONAL TO CLEAN YOUR DEVICE

TIPS TO STAY SAFE	• Maintain strong passwords • Use MFA (Multi-Factor Authentication) • Reboot your computer daily • Check your anti-virus daily, make sure that it is updated with no errors • Engage an IT professional to scan and clean your computer if you notice anything unusual • Be very careful when googling “tech support”, there are many hackers who advertise as IT specialists

Thank you to Scott E. Palmquist from Computer Support Team for providing information for this cybersecurity guide.