BEFORE THE BREACH (INDIVIDUAL)

As an individual, there are several steps you can take to help protect your sensitive data from security threats.

Checklist

Keep software updated.

- ☐ Keep third-party software (inventory, finance, etc.) updated. This could include your web browsers, Adobe, Java, or other software products. Most of these can be set to auto update.

Keep your operating system updated.

- ☐ Enable automatic updates to receive critical patches as soon as they are available.

Download & Install Antivirus Software.

- ☐ Make sure you have the latest version of the software, your virus definitions are set to update automatically, and on-access scanning is enabled. Always download software from reputable sources. Microsoft Windows Defender is free to use.

Use Multi-Factor Authentication wherever possible.

- ☐ Multi-Factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access an online service, such as a website, application or VPN. MFA requires one or more additional verification factors, such as a One Time Pin (OTP), in addition to a password.

Use a password manager to create strong passphrases.

- ☐ Each passphrase should be unique and complex. Use a password manager (LastPass, BitWarden, etc.) to story them securely.

Use a password-protected lock screen.

- ☐ Lock your computer screen before stepping away from it. Press the Windows key + L to lock your Windows computer. To protect your cell phone, enable a passcode and set it to auto-lock.

Protect yourself against phishing scams and identity theft.

- ☐ Always verify the sender of emails or phone calls before providing sensitive information. Never provide your passwords or passphrases to anyone.

Only download software from reputable sources.

- ☐ Only download files, apps, and plugins from trusted sources. Malware, which includes viruses, spyware, adware and other malicious software, can be disguised as or hidden in legitimate software.