CYBERSECURITY CHECKLIST

BEST PRACTICES FOR ALL AGENTS

The following should be implemented throughout your entire office to stay on top of cyberattacks

√ Make sure your **anti-virus** and **anti-malware software** is up-to-date

√ **Back up your data daily** to ensure your data is protected in the event of a ransomware-like attack

√ Practice **network segmentation**

  √ Keep hackers out of your systems by segregating your critical databases and network traffic from your non-private, basic ones

√ Set up **automatic patching** to protect any operating systems or programs from being vulnerable to cyberattacks

√ Set up **multi-factor authentication (MFA)** on your devices

  √ This is a strong defense against cyberattacks as it provides another layer of protection to your credentials and data

√ Set **password policies** to be more than eight characters, containing numbers, special characters, etc.

  √ Consider using **password managers** to digitally store and protect your credentials, avoiding the need to write them down on sticky notes, your phone, or Word/Excel documents

CATIC

building **partnerships** together.

CORPORATE OFFICE
101 Corporate Pl., Rocky Hill, CT 06067 | (800) 842-2216 | www.CATIC.com

CYBERSECURITY CHECKLIST CONTINUED

BEST PRACTICES FOR ALL AGENTS

- √ Utilize **encryption** for your emails and computers to make them near impossible to crack if stolen
- √ Conduct quarterly staff trainings and share weekly security tips to ensure all employees can gain the resources needed to spot and minimize the risk of cyberattacks
- √ Install **firewalls** so you can monitor inbound and outbound traffic based on your own rules
    - √ Consider adding **intrusion detection and/or prevention systems** to your firewall for more enhanced security
- √ Implement **least privilege models**
    - √ Provide only the necessary access to your employees needed to do their jobs (e.g., do not make them local admins on their devices)
- √ Establish a **disaster recovery plan**
    - √ Should your company fall victim to a ransomware attack, the set of tools and procedures you put in place can help in recovering from a cyber nightmare
- √ Set up **spam filters** to block malicious URLs, suspicious attachments, emails outside the U.S., etc.
- √ Practice **application whitelisting**
    - √ Adding/allowing acceptable software that your company deems safe and blocking any unsanctioned applications from running

CATIC

building **partnerships** together.