✓Cybersecurity checklist

- ☐ **Antivirusprogramma** van een gerenommeerde leverancier is geïnstalleerd en geactiveerd op (computer)systemen
- ☐ Minimaal wekelijks wordt een **back-up** van kritische gegevens en/of systemen gemaakt en los van het (computer)systeem opgeslagen
- ☐ **Twee- of multifactor authenticatie** (2FA/MFA) wordt gebruikt om de toegang tot alle web-based (e-mail)accounts te beheren
- ☐ Unieke en veilige **wachtwoorden** van minimaal 12 tekens bestaande uit hoofdletters, kleine letters, cijfers en symbolen worden gebruikt
- ☐ Altijd de meest recente **update** van software, apps en apparaten geïnstalleerd
- ☐ De tekenen van **online fraude en phishing*** zijn bekend en medewerkers zijn hierin getraind
- ☐ Er is een **intern meldpunt** waar medewerkers melding kunnen maken van verdachte e-mails of telefoontjes
- ☐ Er wordt onderscheid gemaakt in **rechten** per medewerker. Dit geldt voor mappen, bestanden en systemen
- ☐ Gevoelige informatie is beveiligd met bijvoorbeeld een **VPN** of een **SSL**

**denk hierbij aan valse e-mailadressen die één teken afwijken, opvallend taalgebruik, het ontbreken van de 's' in de https: van een URL en druk die uitgeoefend wordt om snel te handelen*

VERZEKEREN EN RISICOBEHEER
QUINTES
PART OF THE BROWN & BROWN TEAM