When you work from home, you need to take extra precautions to keep you and your organization safe!

- **Secure your home wireless network** in two ways: use Wi-Fi Protected Access 2 (WPA2) and change the default password to a strong one.

- **Know your organization’s remote work policies** and follow them.

- **Set a strong password or PIN for all devices.** Don’t share work computers or mobile devices with anyone else.

- **Log in with multi-factor authentication** (MFA) wherever possible.

- **Do not use the same password for multiple accounts or devices.** Do use a password manager if one is available. If it’s cloud-based, use MFA to protect your account.

- **Don’t dispose of sensitive data in normal trash.** Follow your organization’s secure disposal policies.

- **IF YOU HAVE HOUSEHOLD MEMBERS OR VISITORS:**
  - Define your physical workspace and communicate boundaries to your household members.
  - Put sensitive information where it can’t be seen accidentally. Keep your desk tidy.
  - Use a privacy screen for your computer and lockable doors and storage spaces when possible.
  - **Lock your screen** when you step away from your computer and/or set an automated screen lock on all devices that contain sensitive data, so if you leave your desk the screen will lock after a pre-set time (such as 20 minutes).

- **Separate your work and personal accounts** whenever possible. Without written authorization from a manager, do not copy sensitive work data to a personal device or upload it to personal email or the cloud.

**Cybersecurity Quick Links**

- vlct.org/cybersecurity
- vlct.org/resource/remote-work-cybersecurity
- vlct.org/resource/pacif-advice-cybersecurity

**VT Agency of Digital Services**
digitalservices.vermont.gov/cybersecurity

Source: LMG Security for Beazley Insurance, Inc., VLCT PACIF’s partner for cyber liability coverage.