VLCM

Work From Home Security Guidelines

Find a quiet place to work and make sure your monitor faces away from any windows or doors.

Don’t use your personal computer for work, and don’t let family members use your work computer.

If you are using Wi-Fi make sure it is encrypted using WPA2 or WPA3.

Use a VPN when connecting to your company's network.

Make sure your wireless router has the firewall enabled.

Contact your internet provider or IT department for help setting up your firewall.

Enable two factor authentication on all your accounts including VPN, applications, computers and network connected devices.

Create long and complex passwords. Long passphrases are better.

- Example: i like to go to the beach and swim in the ocean!
- Don’t reuse passwords

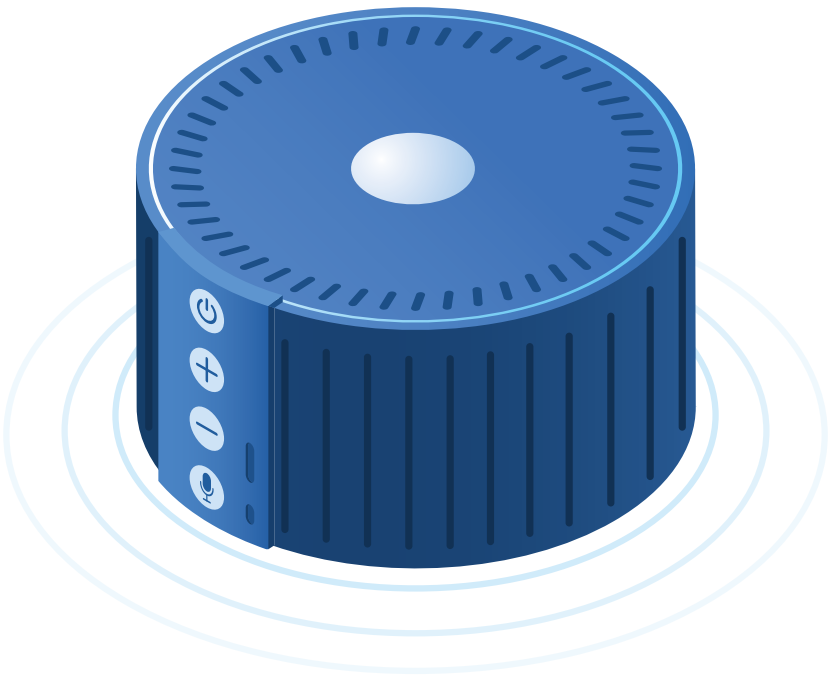
Use a password manager to create and store secure passwords.

Keep your desk clear of any business related or confidential information.

Lock your computer or turn your computer off when you are away from your desk.

Only use employer-approved tools and applications for communicating.

Call your co-worker to verify requests to share confidential information.



Don’t have sensitive or work-related conversations around Alexa, Siri, or Google Home.

Call (don’t email) your IT help desk if you are having an issue with your computer or you think your computer has been compromised.


VLCM