# Remote Work Security Guidelines

Working remotely offers flexibility, but it also introduces new cybersecurity risks that must be managed proactively. As the perimeter of the office network dissolves, each remote workspace becomes a potential entry point for attackers. These guidelines will help you maintain a secure environment while working from home or a public location.

## 1. Secure Your Network

Your home or public Wi-Fi network is not as secure as the corporate network.

- **Home Wi-Fi:**
    - **Change the Default Password:** Your router comes with a default password. Change it immediately to a strong, unique password.
    - **Encrypt Your Network:** Ensure your network is using a strong encryption protocol, such as WPA2 or WPA3. Avoid using older, insecure protocols like WEP.
    - **Change the SSID:** Change the default name of your Wi-Fi network (SSID) to something generic to avoid revealing the router model.
- **Public Wi-Fi:**
    - **Avoid Sensitive Activities:** Never access sensitive information, such as banking or confidential company data, while connected to public Wi-Fi.
    - **Use a VPN:** Always use a company-provided Virtual Private Network (VPN) when on a public network. A VPN encrypts your traffic, making it unreadable to anyone else on the network.

## 2. Protect Your Devices

Your work laptop, tablet, or phone contains sensitive company information and must be protected physically and digitally.

- **Physical Security:**
    - **Lock Your Screen:** Always lock your computer screen when you step away from it.
    - **Keep it Secure:** Store your work devices in a secure location, especially when you are not using them.
- **Digital Security:**

    - **Use Approved Software:** Only install software that has been approved by your IT department.
    - **Keep it Updated:** Ensure your operating system and all applications are kept up-to-date with the latest security patches.

## 3. Handle Data with Care

Data handling is just as important outside the office as it is inside.

- **Data Storage:** Do not save confidential company data to unapproved personal cloud storage services (e.g., Google Drive, Dropbox) or to personal USB drives. Use only approved corporate file-sharing services.
- **Printing:** Avoid printing confidential documents unless absolutely necessary. If you must print, ensure the documents are handled securely and shredded after use.
- **Data on Personal Devices:** Do not transfer company data to your personal computer or other devices unless explicitly authorized and using secure methods.

## 4. Be Cautious of Your Surroundings

Your physical environment matters, especially if you are working from a coffee shop or shared space.

- **Visual Privacy:** Be aware of who is around you. Use privacy screens on your laptop to prevent "shoulder surfing" and ensure no one can see what's on your screen.
- **Audio Privacy:** Be mindful of who can hear you. Avoid sensitive conversations on calls or video conferences in public spaces.

## 5. Report and Communicate

Security is a shared responsibility. If you notice anything suspicious or experience a potential security incident, report it immediately to your manager or IT department. Early detection and reporting can prevent a minor issue from becoming a major incident.