**Date:** [Insert Date]

**To:** [Employee Name]
**From:** [Company Name/IT Security Department]
**Subject:** Remote Work Cyber Liability and Security Protocols

Dear [Employee Name],

As you are working from a home office environment, it is essential to maintain the highest standards of cybersecurity to protect company data and mitigate potential cyber liabilities. This letter outlines the mandatory security requirements for your remote workspace.

**1. Network Security:**
You are required to use a secure, password-protected Wi-Fi network. The use of public or unsecured Wi-Fi for company business is strictly prohibited. When accessing company systems, you must use the approved Virtual Private Network (VPN).

**2. Device Management:**
Only company-authorized hardware should be used for business tasks. Ensure that all software, including antivirus and operating systems, is kept up to date. Do not allow family members or unauthorized individuals to use company-issued devices.

**3. Data Protection:**
Sensitive information must be stored on company-approved cloud drives or servers, not on local physical drives. Password management tools should be utilized, and Multi-Factor Authentication (MFA) must remain enabled at all times.

**4. Physical Security:**
Ensure that your workstation is locked when unattended. Dispose of any physical documents containing company information using a cross-cut shredder.

**5. Incident Reporting:**
In the event of a suspected security breach, lost device, or phishing attempt, you must notify the IT Security Department immediately at [Insert Phone Number/Email].

Failure to adhere to these protocols may increase cyber liability risks and result in disciplinary action. By continuing your remote work arrangement, you acknowledge your responsibility to maintain these security standards.

Sincerely,

[Your Name/Signature]
[Your Title]
[Company Name]