REMOTE WORK:
SECURITY CONSIDERATIONS

As several locations of Cornerstone Building Brands adjust to remote work over an extended and undefined period, we have documented how you can help protect the Company's network resources and its sensitive information while working remotely. Although we have taken steps to secure the network from unauthorized remote access, the unprecedented level of remote work increases the risk that attackers will gain access to the network. You and your actions remain our best defense against these attacks. The goal is to avoid the added disruption and anxiety that would result from a successful cyberattack or loss of sensitive data during this time.

To help minimize risk to the firm's network and data, take these actions while working remotely.

1. Be extra vigilant of phishing emails and other messages that purport to contain some breaking news, surprising information, or other urgent message – especially related to COVID-19 – to entice you to act.
2. Beware of unexpected multi-factor authentication requests. If you receive a request to approve a connection you did not start, **do not** approve the request. Report the unexpected request to your local Help Desk.
3. **Do not** click on untrusted links or open attachments. These links and attachments can be very convincing. If unsure, confirm with the sender by phone or ask your local Help Desk for assistance.
4. **Do not** download or install software from untrusted source or any suspicious emails that may appear to look legitimate. Contact your local Help Desk for assistance.
5. "Remember password" functions should always be turned off when employees are logging into company information systems and applications from their personal devices.
6. Visit only trusted websites for information on the pandemic. Beware of sites advertised in social media posts or sites luring visitors through urgent or inflammatory messages.
7. Because even legitimate sites may become compromised and be used to distribute malicious software, limit unnecessary browsing on company assets. Do not allow family members to use your company equipment for personal use, which can expose the system to unexpected browsing activity.
8. Use only approved solutions to transfer data. Contact your local Help Desk for assistance.
    - For *internal* collaboration and sharing, use approved file-sharing and collaboration tools only.
    - For *external* collaboration and sharing, use approved secure file-transfer or secure encrypted email solution.
    - **Do not** use unauthorized file-sharing sites (e.g., Box, Dropbox).
    - **Do not** email data to your personal email account or transfer data to unapproved portable storage devices.
    - **Do not** email unencrypted sensitive data to external parties. If you send an individually encrypted file, secure it with a strong password, and do not send the password by email.
9. Use only approved conferencing solutions, and ensure your location is secure. Contact your local Help Desk for assistance.
    - For internal and external conferencing, use approved conferencing solutions.

- Ensure that others cannot overhear private conversations when you are working in a shared workspace.

10. Use secure, known networks. Use the company-provided VPN, wherever possible, as the VPN offers an added layer of protection for possible insecure networks.
11. Use a secure password-protected internet connection. Where feasible, verify that Wi-Fi router is protected with the WPA2 or WPA3 encryption setting; ensure your router/modem and internet service provider (ISP) portal are configured with a strong, unique password; and enable software updates for all routers and modems.
12. Report any Company issued lost or stolen devices immediately.

Remember that the ability to work remotely is a privilege, and Cornerstone Building Brands will monitor activity to protect our customers and assets. Your actions and vigilance are critical parts of our defenses. Regardless of work location, employees must adhere to company policies. Violations of company policies and remote work requirements may result in disciplinary action, including revocation of remote work privileges. Refer to Cornerstone IT Policies for additional information on security practices to be adhered to.