CHECKLIST

REMOTE WORK CYBERSECURITY FOR EXECUTIVES & MANAGERS

Cybersecurity-savvy employees are a crucial first line of defense regardless of whether employees are working remotely or in the office. Here are the key things you need to do:

✓ Policies:

Update your policies to take remote work into account. Have all employees that are working remotely review and sign off on any policy changes. Make sure all employees know:

- How to identify sensitive information
- Acceptable practices for handling sensitive information
- Keep work and personal IT resources separate. Don't copy sensitive data to personal accounts or computers unless you have formal written approval.

✓ Training & Awareness:

Provide your staff with regular reminders and awareness training on good cybersecurity practices.

✓ Physical Security:

Physical security while working remotely can be a real challenge.

- Encourage employees to use lockable drawers and rooms to store sensitive data.
- Emphasize the importance of "clean desk" practices in workspaces.
- Remind employees to lock their screen whenever they step away from their computer, particularly if they are in a shared space.
- Consider providing some tools to enhance privacy like a privacy screen for the computer or a physical lock.
- Communicate procedures for disposing of sensitive data while away from the office.

✓ Multi-Factor Authentication (MFA):

Set up MFA whenever and wherever possible. This is especially important for employees that have roles in management, finance, and IT since they are often targeted in scams.

✓ Mobile Device Management (MDM):

Consider installing MDM software for corporate assets, which gives you the opportunity to wipe devices remotely if lost or stolen.

✓ Cloud Download Restriction:

Restrict employees' ability to download documents from the cloud, whenever possible.

✓ Help Line:

Make sure that users have an easy way to report cybersecurity issues, suspicious activity or a lost/stolen device to the appropriate contact.

If you need help defining remote work cybersecurity policies and procedures or testing to check for gaps in your network, contact us, we can help.

LMG™ SECURITY
145 W FRONT STREET
MISSOULA, MONTANA 59802
www.LMGsecurity.com

WE ARE HERE TO HELP

Please contact us any time you have a question or need additional support.
Phone: 406-830-3165 | Toll-Free: 1-855-LMG-8855 | E-mail: info@LMGsecurity.com

REFERRING A CLIENT

To refer a client to LMG Security, please email info@LMGsecurity.com