CHECKLIST

"BRING YOUR OWN DEVICE" (BYOD) SECURITY FOR EMPLOYEES

During this challenging time, many things are not business as usual. You may need to "bring your own device" (BYOD) in order to get your work done—in other words, use your personal computer, phone or tablet for work. How can you keep yourself and your organization secure? Check out this handy list of cybersecurity best practices:

- **Know your organization's policies** for use of personal devices in an emergency. If you are not sure, ask.
- **Put a strong PIN or passcode on every device**
- **Don't share devices unless absolutely necessary.** If you must share a device, give your family members/roommates a different account.
- **Make sure to lock the screen** on your device whenever you leave it unattended.
- **Keep your antivirus up-to-date**
- **Use only approved file-sharing methods if possible.** Do not send sensitive data to your personal email, or upload it to personal cloud repositories such as DropBox or GSuite, without explicit written permission. Doing so can potentially violate contractual or legal obligations and cause long-term consequences for your organization.
- **To the extent possible, don't download or install applications, or surf to web sites that are high risk**, using any devices that you use to store sensitive data. These include many illegal and inappropriate web sites, such as gambling, pornography or gaming sites.
- **Don't download sensitive data to your device** unless you have received explicit written approval. If you can do you work while still leaving sensitive data in the cloud, without downloading it, this is best. Many cloud suites such as Office 365 or G-Suite allow you to edit documents in the cloud without downloading them.
- **Try not to print sensitive data unless absolutely necessary.** When you print a document, a copy of that document is stored in your printer's hard drive, sometimes indefinitely. If you must print a document and have approval to do so, make sure that you physically secure the document.
- **If a device containing sensitive data is lost or stolen, report it immediately** to the designated contact for your organization.

With awareness and education, security can be maintained from wherever work is getting done. Stay healthy and be well!

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