CHECKLIST

EMERGENCY BYOD FOR IT

It's an emergency. You still need to get essential business done. You physically do not have devices to deploy to your staff—but they have their own and are willing to use them for work.

Here are some tips for reducing your risk while enabling employees to use their own devices.

FOR IT STAFF:

- ✓ **Establish a clear policy** for what employees can and cannot do using personal devices. Ensure that this is clearly communicated, both in writing and verbally.
- ✓ **Require a strong PIN or passcode** for all devices.
- ✓ **Implement multi-factor authentication (MFA) whenever possible.** That way, if an employee's home computer is infected with malware and their passwords are stolen, it will be harder for attackers to login to their accounts.
- ✓ **Ensure that all employees have antivirus software installed and updated** on their personal devices. Consider purchasing antivirus licenses for your employees' personal devices that are used for work.
- ✓ **If employees VPN into your network,** consider leveraging VPN tools that scan remote systems and ensure that they meet minimum security standards before connecting.
- ✓ **Restrict employees' ability to download documents from the cloud,** whenever possible.
- ✓ **Take advantage of Mobile Device Management (MDM) features** that are already built into your cloud suites or existing software. Many applications such as G-Suite and Office365 have built-in MDM capabilities, so that you can remotely wipe company data from the employee's device if it is lost or the employee is furloughed.
- ✓ **If you have time and resources, deploy a full-featured MDM** for personal devices so that you can remotely manage and/or wipe your data off of a device if necessary.
- ✓ **Consider purchasing and distributing physical security tools to employees,** such as privacy screens.
- ✓ **Make sure that users have an easy way to report suspicious activity** or a lost/stolen device to the appropriate contact.

If you need help defining work from home cybersecurity policies or testing to check for gaps in your newly expanded 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