REMOTE SECURITY CHECKLIST

In the rush to roll out remote work capabilities, many businesses have left security considerations behind. But with remote workers "in the wild" and unprotected by the company firewall, security is more critical than ever. This checklist can help you guide the conversation about your security needs while ensuring your employees can effectively work remote.

- ☐ Is multi-factor authentication (MFA) enabled? Did employees receive guidance on how to use MFA (and authenticator apps, if applicable)?
- ☐ Is conditional access enabled and configured?
- ☐ Can you remotely wipe company data from lost or stolen laptops and mobile devices? Are you using whole disk encryption to encrypt the physical hard drive of company laptops?
- ☐ Do you have an email security product in place? Were employees trained to recognize and report phishing attempts?
- ☐ Have you installed a web security app to prevent users from visiting malicious sites?
- ☐ Have you set up data loss prevention policies and/or set applicable restrictions on external file sharing?
- ☐ Have you created a remote work and data protection policy for employees to sign?
- ☐ Have you conducted end user training on remote security policies and best practices?
- ☐ Do you have endpoint protection installed for all remote machines?
- ☐ If you are subject to compliance regulations, do you have policies and procedures in place to ensure compliance? Are employees trained to enforce those policies?
- ☐ What is your incident response plan during times of company-wide remote work?

NEED HELP COMPLETING THE CHECKLIST?

DIAMONDIT.PRO | info@diamondit.pro | 661-833-5600