bodman

An Update From Bodman PLC

Bodman PLC | COVID-19 Response Team Website

March 2020

Security Guidelines for Employees Working Remotely

As more businesses allow their employees to work remotely in response to the Covid-19 pandemic, data privacy and cybersecurity risks can become amplified. Employers can mitigate these risks, by considering the remote work guidelines listed below, many of which will serve employers well long after the COVID-19 pandemic has ended.

Remote Work Guidelines

• **Confidentiality Reminders to Employees.** Think about the categories of sensitive information that employees have access to while working remotely (trade secrets, customer lists, employee information, protected intellectual property, etc.), and remind employees of their confidentiality responsibilities with respect to this information. Employers may also choose to determine that remote work will inevitably be less secure, and therefore limit remote workers' access to certain sensitive information.

• **Rules for Use of Personal Devices.** Remind employees to never download or save business information to their personal devices, personal online cloud services, or thumb drives.

• **Rules for Use of Work Devices.** Remind employees that work devices are for employee use only and should not be shared with other household members. Beyond the standard risks of unauthorized persons accessing work systems (access to sensitive information, inadvertent deletion of business records, etc.), non-employee use may introduce new cybersecurity risks to the extent the nature of such use differs from normal business usage. If not already active, businesses should strongly consider implementing two-factor or multi-factor authentication technologies.

• **IT Resources.** A dramatic increase in the prevalence of remote working is likely to stretch IT resources, as new categories of risk emerge and existing ones intensify. Ensure IT professionals are appropriately staffed and trained to address heightened volumes of IT issues, some of which are likely to be novel in nature.

• **Phishing Avoidance.** As noted by the Federal Trade Commission, "scammers are taking advantage of fears surrounding the Coronavirus." Moreover, as employees increasingly use work devices as their primary mode of internet access, the risk of these devices being infected by phishing related viruses grows as well. Employers, therefore, may consider sending anti-phishing reminders or instituting remote anti-phishing training sessions.

• **Hackers.** To be clear, hackers recognize that work at home environments are easier to hack and they may turn their focus to employees working remotely. Employees should ensure that their home routers are secure.

• **Targeted Encryption.** Ensure your most sensitive information (i.e. financial or medical records) is encrypted both in transit and at rest.

• **Update Passwords.** Employers should require employees to utilize strong passwords and require such passwords to be updated frequently.

• **HIPAA.** For HIPAA Covered Entities or Business Associates, remind employees that HIPAA responsibilities continue during this time. For more details on the HIPAA dimension of Covid-19, please see this article in our Bodman Covid-19 Response Team series.

If you have any questions please contact Bodman attorney, **Jill Miller** at 734-930-2499 or jmiller@bodmanlaw.com