Information Governance in the Age of Working at Home: Considerations for Ensuring Data Created by Employees
Working Remotely is Preserved

Your company has successfully tested its capabilities and employees can safely and effectively work remotely from home. Now, hundreds or even thousands of employees across the country may be working remotely and generating and receiving sensitive, confidential and/or proprietary data from their homes. Does your company have policies in place for where that data can be generated and where it must be saved? If so, are those policies enforced? If you don't have policies in place or it has been a while since the policy has been updated, the following are some considerations for information governance when employees are working remotely.

First, is the employee using their own laptop (or other device) for the business-related purposes or are they using a laptop issued by the company? If it is a company-owned laptop, does the laptop automatically get backed up to the cloud or company server or does the employee have to take affirmative steps to back up the data that is created? If the employee must take affirmative steps, it is imperative to make sure that employees are regularly taking those steps for the data to be preserved. Additionally, all company owned laptops should be password protected and should be able to be wiped remotely if the laptop is lost or stolen.

If the laptop or other device is owned by the employee, it can be more difficult to make sure all data is being preserved onto a company-owned platform. If the company allows or requires employees to use their own laptops, consideration should be given to having a remote desktop application or some other similar program that requires an employee to log into a program or application to create and access company-owned materials. Employees should be discouraged or prohibited from creating or copying company-owned documents to their own computer (outside of the application or program). This policy ensures that all company-owned documents are being protected and preserved on company-owned sources. Regardless of whether an application or program is required, all employees who utilize their own laptops for business purposes should be required to have a password (or fingerprint or retina identification) on their laptop so that if the laptop is stolen or lost, all data contained on the laptop is password-protected.

Second, what are your company's "official" methods for both internal and external communication and how are those methods of communication being preserved? For example, employees likely communicate via email. Are those emails being preserved to the cloud or company server pursuant to the company's data preservation and destruction policy regardless of whether those emails are being generated on a company-owned source or one of the employee's devices?

Today, however, employees are likely to communicate with one another (and even employees from other companies) through multiple communication tools, including text messages, collaboration tools such as Slack or Microsoft Teams, and instant messaging tools like What's App. These methods of communications are even more likely when employees are working remotely. Does your company permit these forms of communications for business purposes? If so, how does your company preserve this data, particularly in the case of anticipated or pending litigation? If your policy doesn't address these types of communication tools (or even if they are prohibited), it is important to know if employees are using these tools for business-related communications so appropriate steps can be taken to manage the data. These types of communication tools can be particularly difficult to manage because if your company has a "Bring Your Own Device Policy" for mobile devices, many of these communication tools may only exist on the employee's own mobile device.

With some planning, information governance with employees working remotely is possible. DFL Legal is prepared to assist you by reviewing your current information and data governance policy or by helping you create an information and data governance policy that makes sense for your business needs.

If you have any questions about this issue or any business matter, please contact Samantha Brutout of DFL Legal at sbrutout@dfllegal.com or (412) 926-1816.

DFL|LEGAL
DINGESS, FOSTER, LUCIANA, DAVIDSON & CHLEBOSKI LLP

www.dfllegal.com | 412-926-1800