PUBLICATION

Cybersecurity Concerns when Considering Furloughs

Authors: Alisa L. Chestler
April 6, 2020

Due to the changing and challenging economic circumstances brought on by COVID-19, companies are now having to consider furloughing employees. All companies must consider how they will handle such moves with respect to their information technology infrastructure. The confidential information on IT systems should be protected during this time, especially with regard to customer information, personal information of customers and employees, trade secrets and other confidential information (all "Confidential Information") maintained by organizations. Human resources professionals handling these issues must consult with their management team, including IT, to consider this complex but very significant issue.

In general, we are recommending furloughed employees be disabled temporarily from access to all systems, almost as if they are terminated from employment. Their user accounts can remain intact, but all access should be disabled. This is not to punish employees, but to ensure there is no data leakage. Seem extreme? The concern is that Confidential Information is generally considered "unsecured" when it is accessible by furloughed employees. We also note that independent contractors, temporary staff or others who also utilize corporate resources should also be considered in this process. Of course, any employees who have been laid off should be treated as any other terminated employee and in accordance with an established protocol. If no established protocol has been developed, please consult counsel as soon as possible to ensure all appropriate protective measures have been undertaken and applicable law considered.

Actions to consider taking to protect confidential information and maintain operations:

- Disable all electronic access. This includes email, databases and external vendor platforms (which may require notification to the third parties). Seem extreme? The problem is that information (personally identifiable information, confidential corporate information, trade secrets, etc.) is generally considered "unsecured" when it is accessible by furloughed employees. Distinguishing between employees who you hope will return to service and employees who are not disgruntled can be difficult. It is best to secure in advance.

- Request and obtain all hardware owned by the company (laptops, tablets and cell phones). If you want to allow continued cell phone use, this can be permitted; however, companies should still ensure all access is terminated as noted below.

- Wipe all devices owned by the employee (cell phones, tablets and laptops) and any corporate-owned resources retained by an employee of company email. Generally, this is accomplished through mobile device management (MDM), but not all companies have installed MDM on all portable devices.

- Enable an out of office message so the employee has personal information/personal messages sent to them, but business emails can be redirected to an appropriate resource.

- Determine how or if furloughed employee emails will be monitored to ensure that ongoing work, projects, contractual and legal obligations are not missed.

For specific guidance or more information on this alert, please contact Alisa Chestler, CIPP/US or one of Baker Donelson's Data Protection, Privacy and Cybersecurity Team Members who are ready to help you identify the issues and a plan to mitigate the risks. For more information and general guidance on how to address legal issues related to COVID-19, please visit the Coronavirus (COVID-19): What you Need to Know information page on our website.