KRIEG DEVAULT

Insights

Safeguarding Confidential Information In Remote Work Configurations

March 22, 2020

By: Shelley M. Jackson and Susan E. Ziel

Professionals have been working remotely from their home, their hotel rooms, and even their cars, for years. The COVID-19 crisis caused many of us to significantly increase the number of persons working remotely, the number of hours per day worked remotely, and extent and nature of work being done remotely on very short notice. As organizations adapt to these requirements, we offer this short list of safeguards and reminders to help protect confidential information, manage cyber-liability and protect your organization's reputation.

Mobile Devices. Does your organization have an up-to-date log of all mobile devices that are being used to work remotely, regardless of ownership? Ask all owners/board members, employees, contractors, and any others who may access your organization's systems remotely ("remote workers") to complete and return a short report that (1) lists all devices they currently use, and for each, include a serial number or other identifier that can be promptly available to track a missing device; and (2) affirms the use of all necessary security protections required under your current HIPAA security or other cybersecurity policies (e.g., anti-virus software, strong passwords, secure WI-FI, encryption, etc.).

Confidential Information. Does your organization take steps to protect the various types of confidential information as required by law and/or corporate policies? Several categories merit review, specifically (1) individually identifiable health information in the case of covered entities and business associates under the Health Insurance Portability and Accountability Act (HIPAA); (2) personal information (including sensitive personal information such as social security numbers) regarding, owners/board members, staff, clients, and business partners; and (3) other corporate proprietary information that is not otherwise available to the public. Remote workers who are new to such arrangements should be reminded of these important requirements.

Minimum Necessary Use. Using a principle borrowed from HIPAA, has your organization clarified the specific types of "minimally necessary" confidential information and mobile devices, if any, that your remote workers in various roles require to carry on their remote work? This important question can set expectations and raise awareness at all levels of the organization.

Networks, Software and Apps. Have you communicated a short list of online portals, networks, software programs and applications that are authorized for use by your remote workers to securely access confidential information as part of their remote work? On the flip side, be clear about those programs and apps that are never to be used, including personal email, unsecure WI-FI, social media, consumer cloud storage etc.

Security Reminders. When was the last time you reminded your team about the safeguards necessary to protect the privacy and security of all mobile devices and confidential information used to do remote work? Now is a good time for a refresher, particularly as there may be individuals in your organization working from home who have not previously done so. A helpful item on upcoming Team Meeting Agendas would be

Remote Working Security and might include discussion of the following actions:

- Protect the physical transport of all mobile devices and confidential information, in any form or medium, from one location to another, whether in your personal vehicle, public transportation or otherwise. Maintain personal possession of devices and confidential information at all times; any storage arrangements must be locked and secure at all times;

- Only use secure printing and shredding arrangements;

- Review and follow all corporate policies regarding password strength, auto-logoff features, screen savers, and other security measures;

- Remain vigilant regarding efforts to attempt to compromise security or access confidential information on your remote devices, such as clicking on a phishing email purporting to be from a coworker;

- Delete confidential information stored on smart phones and other devices when it is no longer minimally necessary, ensuring that a retention copy remains available as required and that such deletion does not violate any records retention guidelines or litigation holds;

- Completely shut down and secure the remote work space at the end of each business day or when unattended to ensure secure storage of all devices and confidential information and to limit unauthorized access; and

- Promptly report mobile devices or confidential information that goes missing – whether as a result of a loss, theft or other compromising circumstances –to a designated representative (e.g., Security Officer or otherwise) so to permit prompt investigation, mitigation and correction of any potential security incidents;

- When in doubt, ask – let remote workers know they are always welcome to contact the help desk or other internal IT resource with questions about protecting the organization's confidential information.

We understand demands on organizations have been changing nearly daily and will continue to evolve. Remote work will remain essential, but so too will the many safeguards necessary to protect your mobile devices and confidential information – all for the good of your organization's resources, relationships and reputation. In the coming weeks, please contact us if you have any questions or require additional assistance in managing these important safeguards. While we are also working largely remotely, we have marshalled technology to continue to provide excellent client service throughout this current crisis and stand ready, willing, and able to assist you.