LANE POWELL

March 23, 2020 Publication

Privacy & Data Security in a WFH Environment

COVID-19 Resource

In the midst of widespread societal efforts to slow the spread of COVID-19, companies across industry sectors are moving employees from office environments to work from home setups to promote social distancing. This unprecedented global shift toward remote work puts a new strain on companies' existing infrastructures and policies.

In anticipation of these new challenges, companies across industry sectors should take the following steps:

- Assess the company's data security readiness for increased remote access of information systems.
- Adopt internal privacy policies and data security protocols scaled to reflect company-wide remote work.
- Provide updated employee training on privacy and cybersecurity best practices.
- Ensure that contracts for technology solutions to process or manage company data sufficiently mitigate the company's risk under applicable privacy and data security laws, including HIPAA, Gramm-Leach Bliley and other industry-specific laws.
- Require employees to perform work on secure servers, and to minimize use of hardcopy for work performed and file storage.
- Deploy additional security safeguards as needed, such as arming company laptops with two-factor authentication and encryption for local files.

Some companies may find peripheral benefits in moving toward a remote work model, and choose to continue supporting a remote workforce even when no longer necessary for public health reasons. In these cases, efforts and investments made to address the items listed above will pay dividends when leveraged for long-term implementation.

Topics

COVID-19

Related Practices & Industries

Business
COVID-19 Resource Center
Privacy & Data Security

As your company adjusts in response during these uncertain times, consider getting a complimentary Cyber Health Assessment to evaluate and improve your company's privacy and data security readiness with a primarily remote workforce.