

Information Governance Strategies for When Employees Have to Work from Home

Technology, Privacy, and eCommerce





With locally and nationally mandated lockdowns to curb the spread of the coronavirus, many companies must now require employees to work from home until the pandemic subsides. This raises a number of information governance issues: Will the information and data that employees access

from home be secure? Can they effectively collaborate? Will this come back to haunt companies later during eDiscovery? Can we comply with our records retention requirements?

This hasty shift may tempt companies to give up trying to maintain good information governance strategies until the chaos settles. Instead, companies need to strengthen their information governance, not only to ensure compliance, security, and risk reduction, but also to help their employees be more productive.

Use tools you already have



Applying information governance to employees who work from home requires technology that, fortunately, most companies already own. Platforms like Office 365, Zoom, Slack, or MVision traditionally have been deployed for securing access to applications and intra-department communications.

They can also be applied and implemented to support remote employees. For example, Virtual Private Networks (VPNs), such as Norton Secure VPN or Cisco AnyConnect VPN, allow secure connections from a home personal computer or even iPad back to a corporate repository.

These products need to be configured to ensure that staff can work at home securely, compliantly, and productively. If they aren't already installed on your staff's computers, consider implementing them when everyone returns to the office.

Enabling secure information sharing

Beyond security, the real challenge for working from home is ensuring that information is properly

protected, it’s stored in a secure repository, and can be easily accessed by the designated employees. Instead of saving files and other information on the home personal computers, companies should aggressively enable file sharing to the cloud.

These cloud-based systems, like Box, Perimeter 81, or VMware AirWatch, can support bi-directional syncing from the employee’s personal computer to the cloud. They also make organizing files easier. In addition to tagging and labeling, these systems also have automated classification tools for encrypting or restricting sensitive or confidential information.

Many companies already have Office 365, Google Drive, or other cloud-based information storage. Now is the time to leverage these in-house technologies and implement security and governance controls.

Train, train, train

Even though collaboration tools may already exist in companies’ environments, most users aren't proficient in using them or perhaps even know they exist. When employees are working from home, it is hard to overdo training.

Training can include videos from your vendor, as well as customized training that shows how and where documents are stored on your system. This should also include applying records retention and data security classification policies.

Finally, training should also cover what not to do, including leaving files on drives in home computers or using insecure websites to share information, such as Dropbox.

Companies should also consider establishing collaboration sites for messaging and self-help. These sites can provide links to recorded computer-based training and videos, as well as an updated FAQ page, which should be supplemented with one- or two-page job aids for frequent tasks.

To encourage employee participation, each department could identify “Collaboration Champions” who receive extra training. These champions can create chat channels for informal peer-to-peer help within a department.

Final thoughts

Information governance strategies help companies ensure their information is secured, managed, and compliant. Perhaps more importantly, these collaboration strategies help ensure that information is accessible both within and across departments, especially when employees work from home.

Faced with the sudden challenge of the entire staff telecommuting during this pandemic, companies should not put off good information governance. Rather, they should accelerate it. Not only for compliance and risk reduction, but to ensure employees can remain productive, engaged, and collaborative.

Visit ACC's COVID-19 Resource Center for more legal best practices on the coronavirus pandemic.

Mark Diamond



CEO and Founder

Contoural Inc.

Mark Diamond is the CEO and founder of Contoural Inc., an independent provider of information governance consulting services. His company works with more than 30 percent of the Fortune 500, plus many mid-sized and smaller companies.