RISK INSIGHTS Technology

ECBM EFFECTIVE COST BASED MANAGEMENT INSURANCE BROKERS & CONSULTANTS

Keys to a Secure Remote Work Program

Allowing employees to work remotely from home or other off-site locations can increase productivity for workers, reduce costs for the company and create beneficial flexibility to keep operations going if something happened to your business's primary physical location. However, remote work, or telecommuting, needs to be conducted carefully with the help of established company policies to protect workers, your clients and your company.

Balancing the Benefits

For the organization, one of the most tangible benefits of remote workers is the decrease in costs associated with having on-site employees. Workspace real estate can be reduced or kept at current levels, while still allowing your staff to grow. Companies can reduce utility expenses, reducing their overall carbon footprint. In addition, your employees can enjoy a savings on fuel expenses, vehicle maintenance and meal costs.

Many employees flourish in a remote work situation. The flexibility it allows can increase morale and help balance work and home life, resulting in increased productivity. As well, remote work options allow a company to employ talent from all over the world.

Having employees in different locations and able to work at home also increases your business's ability to continue operations in the event of a disaster. If for some reason your physical office had to close, many business functions could still go on.

Start Small

Begin your remote work program on a small scale using a pilot program. Present the opportunity to just one or a few established employees whose work could be well-suited for this type of environment, even if troubles are met along the way. Testing this program before a company-wide implementation will help address the inherent risks to business processes and workflows as bumps along the way, rather than wide-spread problems.

While remote work can pose many exposures, most of them can be mitigated with thorough planning and proper execution. Once policies and procedures are established, companies can take full advantage of the benefits that having remote workers offers.

Remote work needs to be conducted carefully with the help of established company policies to protect workers, your clients and your company.

Project Productivity Risk

The change in environment will mean that workflows will need to be adjusted. As well, different methods of communication and oversight will need to be used to keep supervisors and team members just as connected to remote workers as they are to the workers in the workspace next to them. Employees allowed to work remotely should already be in good standing with the company and understand what it will take from them to keep projects moving. Overall, with the right adjustments, productivity should remain the same, if not improve, for remote workers.

Keys to a Secure Remote Work Program

Safety at Home

Workplace safety and ergonomics should be just as important for remote workers as on-site workers at your company. Remote workers should attend a specialized safety training or orientation to thoroughly address all possible exposures they'll face in their new environment, including ergonomics.

When a remote worker begins in their new workspace a site visit should occur with a supervisor or HR personnel to check that all commonsense safety measures are being addressed. Periodic visits are a good idea to ensure continued compliance. Remember that remote workers have all the same rights to workers' compensation for injuries that occur in the course of employment that employees in your facility do. Not monitoring a remote workers workspace periodically can allow hazards to develop, putting your company at greater risk for a workers' comp claim.

Information Security

Information security is the largest challenge for companies with remote workers. Physical loss or theft of devices containing data or access to data is much more likely. Remote workers will usually be in possession of laptops and/or mobile data drives issued by the company to allow them to work with the same systems and information as workers located in-house. The protection of building security, key cards and the watching eyes of other employees will not be able to protect their equipment.

Another aspect of security to be cautious about is using company-issued equipment for non-work related tasks. If laptops are accessed by family members they could potentially download a virus or spyware. The same could happen if an employee got lax and used their company equipment for personal use. Companies should also be aware of how any sensitive data or documents will be stored and disposed of. Physical print outs especially need to be disposed of properly.

To protect your employee and your company's interests, be sure that all equipment requires passwords and encryption for access. A thorough policy should be established regarding the line between personal and company property and activity for remote workers to prevent missteps from happening. When establishing the employees remote worksite, be sure that any wireless connection is secured and that your company has a policy about using unsecured connections (such as at hotels and other public spaces) for work tasks. Companies can also set up VPN (Virtual Private Network) access for connecting to the company's networks, to ensure that access is secure.

Contact ECBM, LP for more information on protecting your business's best interests and planning for business continuity and growth.