Tips On What Your Confidential Information Policies Must Have

Confidentiality at work has become increasingly important and the employee's responsibility to keep private and confidential information is just that, private and confidential. Questions from employers about what must go into this type of policy have become routine, mainly due to the global nature of communications today and how easily information can be circulated and accessed. Before we say what we think is most important in general terms, the objective of this type of policy should always be to keep information private and confidential. The exact nature of a policy will vary based on the needs of your business. For example, a health care setting may have a much more detailed confidentiality policy than a toy store, but all organizations need these types of policies to protect themselves in a competitive business environment. Having a policy in place is one of the many steps required to have a dispute-free workplace.

With that in mind, here's what we see as key to your business information remaining private and confidential.

Tip 1- Clear definitions

Employees must know what information they can access and what information must remain private and confidential. Pay close attention to the definition section of your policies to make sure employees are aware of their limits. It is very important for employees to know what actions are considered breaches of confidentiality. Spell out in detail what you mean by "confidential information" or "private information". Don't borrow someone else's definition of "confidential information" or "private information"; tailor it to the particular needs of your business. If you're not clear, you're leaving the door open to an "I didn't know" defence.

Tip 2 – Communication and documentation is key

Once your policy is ready, communicate it to ALL employees, including supervisors and managers. Provide further training by holding meetings and training sessions where attendance is noted, copies of the policy are distributed and those in attendance have an opportunity to read the policy. Encourage questions and provide clear answers. If you don't communicate, you're leaving the door open to a "nobody told me" defence.

Tip 3 – Spell out the consequences

Along with knowing what a breach is, employees MUST know what the consequences of a breach will entail. If they don't know they will be disciplined, they can argue down the road that they were not aware that they would be suspended or terminated for their actions. Make it clear that any breach will result in discipline. If you don't set forth the consequences, you're leaving the door open to an "I didn't know I would be fired" defence.

Tip 4 – Return property on termination

Although it might seem obvious, this is a very important component of this type of policy. It is essential to specifically state that employees must return all company property on termination. Although it might be stated in your policies elsewhere, if it's not included here what's to stop an employee who has had a laptop with private and confidential information on it to just say "I thought it was a perquisite" defence.

Tip 5 – It doesn't end here – continuing obligations

Even after the employment relationship ends, an employee may have continuing obligations to a former employer. In other words, the duty to protect private and confidential information does not simply end with employment. In the policy, make it clear that it doesn't end and include language that you will take steps to protect the information in such circumstances.

What this means for employers

Following these tips will emphasize and stress fundamental employee obligations and duties. Along with other provisions in your policy, knowledge and awareness of these rules can limit careless disclosures and, ultimately, limit liability itself. When employees know the rules and consequences of a breach, the more seriously they will take their duties and obligations. If confidential information does get disclosed, you will have already taken a big step towards defending the business and providing the documentation you need to protect your business.

Last Updated: August 2 2014

Article by Grant G. Machum and Alison Strachan

Stewart McKelvey