5 Policies Employers Need to Protect Their Business

www.colemantechnologies.com

COLEMAN TECHNOLOGIES

It is always essential to keep your employee policies up-to-date. This year is no exception. Every company deals with work-at-home issues, cybersecurity threats, and online data issues. These turbulent times cause most employers to change the way they manage their companies and employees. We have compiled five of the top policies to update at this time. We're sure you'll find many more.

1 Updated Employee Separation Procedures

The switch from office-based work to working at home can create uncertainty and chaos within an organization. Many etched-in-stone policies like paid-time-off, family leave, and other vital benefits become a bit fuzzier when your employees do all their work at home. Family responsibilities like child-care and at-home chores often eat into the workday. On the positive side, staying home does have benefits. No more long, crazy commutes, no conferences or trade shows and virtual meetings mean fewer expenses and more time available to work.

Employee separation policies can be unclear with so many remote workers. How do you 'walk somebody out'? What do you do with their company laptops? What are your employees doing with company data? Insider threats are a growing problem for IT managers. Having a clear separation policy will ensure your employees understand their obligations to return assets if they decide to change jobs.

2 Updated Password Policies

Remote workers can pose several threats to a business. Home computer networks are rarely as secure as an on-premise network. The use of cloud-based software means employees must maintain and remember dozens of different passwords. One proven way to manage passwords is by using a password management tool provided by your IT department or managed service provider. We also recommend ending the practice of rotating passwords unless there is a suspected password compromise.

3 Use Multi-Factor Authentication

It is difficult to confirm the identity of remote workers when they are logging into corporate applications. Updating your identity administration policies and using multi-factor authentication (MFA) will improve password security procedures. MFA requires employees to confirm their identity by entering a unique passcode sent to their email or mobile device. Mobile authentication apps for IOS and Android devices simplify the verification process.

4 Cybersecurity Incident Response Plan

Cyber attacks are on the rise, and small businesses are often the victims of data breaches and ransomware attacks, which can disrupt business operations. Updating your cybersecurity incident response plans will allow your employees to quickly respond to attacks and use strategies like on- demand data backups and other disaster recovery plans to bring the company back online. While these policies directly affect the IT department's actions, they also instruct all employees on the steps they need to restore business applications and customer data.

5 Data Storage Policy

Many businesses have a combination of on-premise and cloud-based data storage systems. Both types of systems require detailed data storage policies. Personal Health Information (PHI), customer data and transaction/contract data all need to meet strict compliance regulations. Policies need to spell out these reporting requirements.

Expert Employee Policy Services

Updating your employee policies can be an intimidating process, especially for IT-related topics. If you don't have the internal resources to handle this critical process, you should consider turning to an expert partner. Coleman Technologies is the expert IT partner you need to identify and write updated employee policies. *Visit the Coleman Technologies website* or call them at **(604) 513-9428.**