6 Security Policies Washington DC Businesses Should Consider

Posted on Sep 28, Posted by Ira Greene Category IT Blog

Security is an important aspect to a company's continuity, and while portions of business security involve things like anti-virus and firewalls, other aspects of security can't be handled by a piece of equipment. In these cases, your organization needs to create security policies, and keep them up to date as the company grows and changes. There are many policies and sub policies that are necessary for any organization that, if non-existent, can cause chaos down the road.

Acceptable Use Policy

This policy is a pretty straightforward set of rules that define what is allowed and what is not allowed on company equipment and resources. Typically the Acceptable Use Policy covers things that are prohibited and the consequences received, such as software pirating or accessing inappropriate web-content. The Acceptable Use Policy isn't designed to make employees feel like prisoners however, it just sets the boundaries for productive and acceptable work habits. For example, you may allow employees to make send text messages or use Facebook as long as it doesn't interfere with day-to-day business and work still gets done.

Password Policy

Password policies can typically be set up on your server to enforce a minimum length and the types of characters required in the password. This policy can also dictate how often passwords need to be changed. It is also a good idea to tack on a number for how many unsuccessful login attempts are made before the account is locked out.

Storage and Retention Policy

Data, both digital and hardcopy, can pose a security risk when not archived and organized properly. These policies detail things from file structure to how long certain data is retained. Some industries have their own sets of laws for data retention, for example a legal office may be required to keep customer records for a certain number of years. When possible, it's recommended to go beyond the minimum requirement and have better than the recommended security just to be on the safe side. Data backup plays a huge role in this policy, and it is important to have a structured plan in the event of a disaster or hardware malfunction.

Privacy Policy

It is important to clearly define what information is considered private and what data is not considered private. You will want to enforce privacy that at least complies with legal regulations, which may vary depending on your business. Privacy Policies include data collection as well.

Incident Response Policy

This is the emergency policy. Just like you should prepare for bad weather with flashlights and batteries, preparing for a security incident should be done in advance. The policy should cover multiple types (or levels) of instances and how to handle each. Address the basics such as hardware outages, data theft, data leaks, and failure to comply with other policies. Proper planning and definition will keep downtime to a minimum.

Social Media Policies

This policy is an offshoot of the Acceptable Use Policy and the Privacy Policy that involves social media and online behaviors. Businesses need to clearly define what is appropriate and inappropriate behavior on the internet. The goal of this isn't to prevent employees from using social media, and doesn't need to abolish all content related to the company; social media is a huge marketing paradise for small businesses. The policy should define what is acceptable, what type of information can be shared, and lay out actions and activities that are not appropriate, such as portraying the company negatively or leaking private information.

If your security policies aren't laid out and organized, or they aren't kept up to date with regular revisions as the company changes and grows, you risk potential chaos, customer dissatisfaction, and worse, legal issue. Have a suggestion to add for other Washington DC small businesses? Let us know in the comments!

Tags: Tagged in: Security Small Business Social Media