

## TOP 5 TIPS FOR DEVELOPING AN EFFECTIVE COMPUTER USE POLICY

By Jillian Swartz  
September 18, 2018

**“A carefully-drafted AUP is one of the best ways for organizations to reduce the likelihood that their computer systems will be used for illegal, discriminatory or other improper purposes.”**

As technology becomes more pervasive and employees spend an increasing part of their work day on the internet and checking their social media feeds, every organization should develop an acceptable use policy (AUP). A carefully-drafted AUP is one of the best ways for organizations to reduce the likelihood that their computer systems will be used for illegal, discriminatory or other improper purposes. This article offers my top 5 tips for creating an effective AUP.

### 1. The Key Elements

A strong AUP communicates an organization’s values and describes, in clear terms, how employees are expected to use the organization’s computer systems. In addition, a properly developed and implemented AUP supports consistent treatment of employees, ensures transparency and offers a measure of protection from claims against the organization. A robust AUP should address topics such as (i) permitted and prohibited uses, (ii) security measures and passwords, (iii) email usage, (v) use of social media, and (vi) consequences for failure to follow the policy. It should also clearly state that the organization’s computer system (including any electronic device that is used for business purposes) is owned by the organization and therefore, the organization has the right to monitor employees’ use of the computer system.

### 2. Start with the Right Team

In order to create an effective AUP, it is important to create a steering committee that is responsible for developing the policy. The steering committee should be chaired by the executive sponsor, who is a member of senior leadership who will champion the policy, and comprise employees who

FOLLOW US:

[AMSBIZLAW.COM](http://AMSBIZLAW.COM)



possess a broad range of perspectives, including employees with IT, risk, legal, human resources and marketing backgrounds. It is important to note that the most effective AUPs are developed by committees that include employees from all levels within the organization. Where employees are engaged in the development of the policy from the very beginning, it is more likely that they will follow the policy.

### 3. Training

A compelling launch of the AUP is critically important to obtain “buy in”. When the executive sponsor of the AUP hosts a town hall to explain what the policy covers, why it was developed, and how it was developed, he or she is setting a clear tone. Where senior leadership demonstrates a sincere interest in, and commitment to, the AUP, employees are more likely to comply with it.

Once the AUP has been formally launched, it is important to ensure that all employees are properly trained. Participation in training should be documented in each employee’s human resources file. Following the initial launch of the AUP, organizations need to be mindful that employees should participate in refresher courses and each new employee should receive training as part of his or her on-boarding process. Regular training keeps the policy front of mind and helps to develop a culture of compliance. In addition, on-going training and communications about the policy will be a good investment in the event that disciplinary action against an employee for breach of the AUP is necessary.

### 4. Enforcement

Consistent enforcement of the AUP is imperative. It is far worse to have an AUP that is not enforced than it is to have no policy at all. For example, if an executive or a top sales person breaches the AUP and the organization does not enforce the policy because he or she is deemed too important to discipline, the organization is sending a clear message that certain people are exempt from the policy and compliance will likely plummet.

### 5. On-going Review

On-going review and updating of the AUP is key in order to ensure that new technologies, risks and workplace practices are properly reflected. An AUP that is a “live document” will be more effective than one that is left on the shelf gathering dust until a data breach or other significant event occurs.

## Conclusion

In order to ensure that an organization has an effective AUP, it is important to ensure that the AUP is clear about the types of computer usage that are permitted and prohibited, the development of the policy involves a broad range of employees with different perspectives, employees receive appropriate training on the policy, the AUP is consistently enforced, and the AUP is kept up-to-date.

The lawyers at Allen McDonald Swartz LLP have significant experience advising organizations with respect to IT policies, privacy policies and Canada's Anti-Spam Legislation. If you need more information about developing your technology policies, please contact Jillian Swartz by phone at 416.262.8206 or by email at [jswartz@amsbizlaw.com](mailto:jswartz@amsbizlaw.com) or any other member of the AMS team.

Allen McDonald Swartz LLP periodically provides materials on our services and developments in the law to interested persons. The information and the comments herein are for the general information of readers and are not intended as legal advice or opinions to be relied upon in relation to any particular circumstance. For guidance on the application of the law to particular situations and circumstances, readers should seek professional advice.

Please contact the author for permission to reproduce, display or reprint this article.



**ALLEN MCDONALD SWARTZ LLP**  
Business Lawyers



**Canada's Top 10  
Corporate Law Boutique**  
*Selected by Canadian Lawyer Magazine*

[WWW.AMSBIZLAW.COM](http://WWW.AMSBIZLAW.COM)